

Aalto University
School of Science
Degree Programme in Security and Mobile Computing

Ashok Rajendran

Security Analysis of a Software Defined Wide Area Network Solution

Master's Thesis
Espoo, July 13, 2016

Supervisors: Professor Tuomas Aura, Aalto University
 Professor Markus Hidell, KTH Royal Institute of Technology

Advisor: Pekka Isomaki, M.Sc. (Tech.)

Aalto University
School of Science
Degree Programme in Security and Mobile Computing

ABSTRACT OF
MASTER'S THESIS

Author:	Ashok Rajendran		
Title:	Security Analysis of a Software Defined Wide Area Network Solution		
Date:	July 13, 2016	Pages:	71
Major:	Data Communication Software	Code:	T-110
Supervisors:	Professor Tuomas Aura Professor Markus Hidell		
Advisor:	Pekka Isomaki, M.Sc. (Tech.)		
<p>Enterprise wide area network (WAN) is a private network that connects the computers and other devices across an organisation’s branch locations and the data centers. It forms the backbone of enterprise communication. Currently, multi-protocol label switching (MPLS) is commonly used to provide this service. As a recent alternative to MPLS, software-defined wide area networking (SD-WAN) solutions are being introduced as an IP based cloud-networking service for enterprises. SD-WAN virtualizes the networking service and eases the complexity of configuring and managing the enterprise network by moving these tasks to software and a central controller. The introduction of new technologies causes concerns about their security. Also, this new solution is introduced as a replacement for MPLS, which has been considered secure and has been in use for more than 16 years. Thus, there is a need to analyze the security of SD-WAN, which is the goal of this thesis.</p> <p>In this thesis, we perform a security analysis of a commercial SD-WAN solution, by finding its various attack surfaces, associated vulnerabilities and design weaknesses. We choose Nuage VNS, an SD-WAN product provided by Nuage Networks, as the analysis target. As a result, many attack surfaces and security weaknesses were found and reported, especially in the Customer Premises Equipment (CPE). In particular, we found vulnerabilities in the CPE’s secure bootstrapping method and demonstrated some attacks by exploiting them. Finally, we propose mitigation steps to avoid the attacks.</p> <p>The results of this thesis will help both the service provider and the SD-WAN solution vendor to know about the attack surfaces and weaknesses of SD-WAN before offering it to their customers. We also help in implementing the temporary countermeasures to mitigate the attacks. The results have been presented to the service provider and the vendor of the SD-WAN product.</p>			
Keywords:	SD-WAN, Nuage VNS, virtual network functions, security analysis, VXLAN, SDN overlay, man-in-the-middle attack, API access control		
Language:	English		

Aalto-universitetet
Högskolan för teknikvetenskaper
Examensprogram för datateknik

SAMMANDRAG AV
DIPLOMARBETET

Utfört av:	Ashok Rajendran		
Arbetets namn:	Säkerhet Analys av Software Defined Wide Area Network Lösning		
Datum:	Juli 13, 2016	Sidantal:	71
Huvudämne:	Datakommunikationsprogram	Kod:	T-110
övervakare:	Professor Tuomas Aura Professor Markus Hidell		
Handledare:	Pekka Isomaki, M.Sc. (Tech.)		
<p>Enterprise wide area network (WAN) är ett privat nätverk som förbinder datorer och andra enheter över en organisations gren platser och datacenter. Den utgör ryggraden i företagets kommunikation. För närvarande är Multiprotocol Label Switching (MPLS) används ofta för att tillhandahålla denna tjänst. Som en ny alternativ till MPLS, mjukvarudefinierad wide area nätverk (SD-WAN) lösningar införs som en IP-baserad molnnätverkstjänst för företag. SD-WAN virtualiserar den nätverkstjänst och underlättar komplexiteten i konfigurera och hantera företagets nätverk genom att flytta dessa uppgifter till programvara och en central styrenhet. Införandet av ny teknik medför oro om deras säkerhet. Dessutom är den nya lösningen infördes som en ersättning för MPLS, som har ansetts säker och har använts i mer än 16 år. Det finns således ett behov av att analysera säkerheten i SD-WAN, vilket är målet med denna avhandling.</p> <p>I denna avhandling vi utför en säkerhetsanalys av ett kommersiellt SD-WAN-lösning, genom att hitta de olika attacktytor tillhörande sårbarheter och svagheter konstruktions. Vi väljer Nuage VNS, en SD-WAN produkt från Nuage Networks, eftersom analysen mål. Som ett resultat, blev många attacktytor och svagheter i säkerheten och rapporteras, särskilt i Customer Premises Equipment (CPE). Framför allt har vi hittat sårbarheter i CPE säkra bootstrapping metod och visade vissa attacker genom att utnyttja dem. Slutligen föreslår vi begränsnings åtgärder för att undvika attacker.</p> <p>Resultatet av denna avhandling kommer att hjälpa både tjänsteleverantören och SD-WAN-lösning leverantör för att veta om de attacktytor och svagheter i SD-WAN innan erbjuda det till sina kunder. Vi hjälper också att genomföra de tillfälliga motåtgärder för att mildra attackerna. Resultaten har presenterats för tjänsteleverantören och leverantören av SD-WAN produkt.</p>			
Nyckelord:	SD-WAN, Nuage VNS, virtuella nätverksfunktioner, säkerhetsanalys, VXLAN, SDN overlay, man-in- the-middle attack, API åtkomstkontroll		
Språk:	Engelska		

Acknowledgements

First, I want to thank my supervisor, Prof. Tuomas Aura for his guidance throughout my thesis work. I am thankful for the time he has spent on discussing my topic and on guiding my work. I am grateful to my instructors, Mr. Isomaki Pekka and Mr. Janne Mikola from Sonera for providing me a chance to work on the latest technology for my thesis and also helping me in understanding the new concepts.

I would also like to thank my supervisor, Prof. Markus Hidell for providing me a remote support for finishing my thesis. Finally, I would like to add a word of gratitude to my friends and family for supporting me throughout my master study.

Espoo, July 13, 2016

Ashok Rajendran

Abbreviations and Acronyms

SD-WAN	Software Defined Wide Area Network
SDN	Software Defined Networking
NFV	Network Function Virtualisation
NV	Network virtualisation
VNS	Virtualised Networking Services
VXLAN	Virtual Extensible Local Area Network
MPLS	Multiprotocol Label Switching
CPE	Customer Premises Equipment
VPN	Virtual Private Network
IPsec	Internet Protocol Security
ATM	Asynchronous Transfer Mode
DSL	Digital Subscriber Line
IETF	Internet Engineering Task Force
WAN	Wide Area Network
LAN	Local Area Network
OPEX	Operational Expenditure
NAT	Network Address Translation
VLAN	Virtual Local Area Network
GRE	Generic Routing Encapsulation
ONUG	Open Networking User Group
PKI	Public Key Infrastructure
CA	Certification Authority
API	Application Program Interface
NSG	Network Services Gateway
VSC	Virtualized Services Controller
VSD	Virtualized Services Directory
VSP	Virtualized Services Platform
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
XMPP	Extensible Messaging and Presence Protocol

MP-BGP	Multiprotocol Border Gateway Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
OF-TLS	OpenFlow over Transport Layer Security
HTTPS	Hypertext Transfer Protocol secure
XML	Extensible Markup Language
SSH	Secure Shell
TLS	Transport Layer Security
SNMP	Simple Network Management Protocol
TEK	Traffic Encryption Key
NTP	Network Time Protocol
SEK	Seed Encryption Key
AES CBC	Advanced Encryption Standard cipher block chaining
HMAC	Hash-based message authentication codes
GUI	Graphical User Interface
TCP	Transmission Control Protocol
SS7	Signalling System No. 7
SSL	Secure Sockets Layer
CSR	Certificate signing request
MITM	Man-in-the-middle
DOS	Denial of Service
TPM	Trusted Platform Module
EK	Endorsement Key
SRK	Storage Root Key
SHA-1	Secure Hash Algorithm 1
RSA	Ron Rivest, Adi Shamir and Leonard Adleman Algorithm
BGP	Border Gateway Protocol
AAA	Authentication, Authorization and Accounting
UID	Unique Identification Number
XMPP-TLS	Extensible Messaging and Presence Protocol over Transport Layer Security

Contents

Abbreviations and Acronyms	5
1 Introduction	9
2 Background	13
2.1 Enterprise networks	13
2.2 Existing MPLS-based networking solution	14
2.3 Problems faced with MPLS	15
2.4 Cutting-edge technologies	16
2.5 SD-WAN solution	19
2.6 Need for security analysis of SD-WAN solution	20
2.7 Related literature	22
3 Case study:Nuage VNS solution	24
3.1 Nuage VNS architecture	24
3.1.1 Nuage VNS operation	27
3.2 Nuage VNS security features	28
3.2.1 Interfaces of Nuage VNS	28
3.2.2 NSG and the bootstrapping process	30
3.2.3 Control plane security: VSC security	32
3.2.4 IPsec key rotation method	32
4 Vulnerabilities and attack scenarios	35
4.1 Analysis of NSG attack surfaces	35
4.2 Basic vulnerabilities	38
4.2.1 Vulnerability 1: open SSH port	38
4.2.2 Vulnerability 2: open HTTP port	40
4.2.3 Vulnerability 3: activation e-mail	40
4.3 Attacks against the NSG bootstrapping process	43
4.3.1 NSG bootstrapping process	44
4.3.2 Man-in-the-middle attack	47

4.3.3	Insufficient access control to APIs	49
4.3.4	Other attacks	53
5	Discussion	54
5.1	Solutions for the attacks	54
5.1.1	Minimizing NSG's attack surface	54
5.1.2	Replacing the bootstrap CA certificates	55
5.1.3	Adding secure access control at the proxy	55
5.2	General discussion	56
5.2.1	TPM	56
5.3	Future work	57
6	Conclusions	59
A	Accessible APIs	66
B	Client certificate authentication	68
C	Snapshots of the MITM tool	70

Chapter 1

Introduction

Enterprise networks form the backbone of everyday communication that connect computers and other devices across different company branches including data centers. These networks allow users and devices in the enterprise network to share data in a secure way. Such enterprise networks may include Wide Area Networks (WAN) and Local Area Networks (LAN), depending on the organization structure and operational requirements. In the early days, point-to-point leased lines were used to provide enterprise network solutions with dedicated DS0 and T1/E1 or T3/E3 connections [10]. In the 90s, this was replaced by the less expensive frame relay service, which required fewer physical connections. Thus, this technology was widely accepted by many enterprises including banks. MPLS is the successor to the frame relay service. It was designed as an IP based solution to use the infrastructure of a telecom network. Hence, telecom service providers prefer the MPLS based solution over the frame relay service to offer for their customers. For instance, Sonera, a leading telecom operator in Finland, currently offers an MPLS solution called as Sonera Datanet, and it is a market leader in Finland.

In spite of having been adopted by many enterprises, MPLS has its drawbacks in terms of cost and bandwidth. MPLS connections remain expensive and offer low bandwidth compared to the public internet. Moreover, the introduction of technologies such as IPsec VPN allows sharing of enterprise data over the public internet in a secure way. Considering the above factors, enterprises started to look for alternative solutions to MPLS. On the other hand, service providers also face problems in providing MPLS to the new generation enterprises which have started to rely on public clouds for their infrastructure. MPLS has problems in connecting the enterprise branch sites to the public clouds operated in third-party data centers. Due to this business shift, Sonera has started to see a decline in revenue in its MPLS business recently. Consequently, there is a need for both enterprises and

service providers to look for a new solution.

The Software Defined Wide Area Network (SD-WAN) solution is introduced as a new generation of enterprise networking in order to overcome the above mentioned problems. SD-WAN is an internet and SDN based, cloud-networking service offered to the enterprises. It virtualizes the networking service and eases the complexity of configuring and managing the enterprise networks.

The introduction of new technologies causes concerns about the underlying security model and robustness of the new product implementations. Also, this new solution is introduced as a replacement for MPLS, which has been considered secure and has been in use for more than 16 years, despite many targeted attacks¹. This makes it a necessity to analyze the security of the SD-WAN architecture and products before wide scale deployment. This thesis is about studying the security model of SD-WAN by performing an in-depth analysis of a commercial SD-WAN product called Nuage VNS offered by Nuage Networks. Following a responsible disclosure process, we have reported all discovered vulnerabilities to Nuage Networks. The vendor has responded in a very constructive way, and we expect the issues to be solved. This work has been carried out at Sonera, Finland, as part of Business Defined Networking team, which offers SD-WAN solution to Finnish enterprises.

Research problem

Our goal is to perform *thorough security analysis of a SD-WAN solution, which includes finding its various attack surfaces, associated vulnerabilities and design weaknesses and then demonstrate attacks that exploit found weaknesses. The ultimate goal is to propose solutions and mitigation steps to avoid any attacks.* We aim to achieve the following things:

1. Understand the architecture and operations of a SD-WAN solution in order to perform security analysis on it.
2. Identify the attack surfaces and security weaknesses in that solution.
3. Demonstrate attacks based on the found weaknesses and evaluate the significance and criticality of each attack.
4. Find possible solutions, mitigation steps and propose design changes to improve the security of the SD-WAN solution.

¹<https://securityintelligence.com/enterprise-attack-it-security-need-risk-based-layered-security-strategy-defend/>

Research methods

We theoretically analyze the security requirements of SD-WAN solution based on the white paper [27], released by ONUS SD-WAN working group. Then, we conduct a case study by taking one SD-WAN product available on the market. Subsequently, in-depth testing is carried out on that solution to confirm that the solution meets the security requirements. In the course of our testing, we implement many attacks based on the weaknesses found in the analysis. This thesis uses a case study approach where a particular person, situation or solution is studied in order to understand a principle in general [35]. Thus, we study and analyze Nuage VNS security in detail in order to understand SD-WANs security in general. Moreover, in security research it is common to focus on attacks in order to understand the threats against new technology and security requirements. The results help us to harden the technology against potential future attacks.

Impact and sustainable development

SD-WAN is introduced as a new, advanced solution for providing enterprise networking. Our thesis focuses on SD-WAN and it helps in identifying and evaluating its weaknesses, which will help in improving its security. Specifically, it helps the service providers to understand the SD-WANs security concerns before offering it to their customers. Thus, it will have an impact on SD-WAN's wide-scale deployment, which in turn will have an effect on the economic sustainability of service providers. Once SD-WAN has been accepted and deployed globally, this thesis work will contribute to the global sustainable development of enterprise network services. Further, this thesis brings ethical impacts to the society by revealing the threats and attack surfaces, which might have been exploited by the criminals to attack the enterprise network and incur losses. We believe that through this research work, the device vendors can see the significance of the threat and will make an effort to mitigate it. As engineers working to deploy new innovative technology, it is our responsibility to ensure its information security before deployment to critical enterprise systems.

Structure of the Thesis

This thesis is divided into six chapters including this introductory chapter. Chapter 2 gives an overview of enterprise networking and its current solution,

MPLS along with its disadvantages. Then, the architecture and working of an SD-WAN solution is discussed. Finally, we list the related literature, which is used as a starting point for our security analysis. Chapter 3 introduces the SD-WAN product, Nuage VNS, offered by the Nuage Networks. We study its architecture and operation in this chapter. Further, we also look into the available security features in Nuage VNS and discuss the results of our analysis on them. Chapter 4 presents the vulnerabilities found in the Nuage VNS in our detailed analysis. We exploited some of the weaknesses and performed attacks on Nuage VNS, which is also explained in detail. In chapter 5, we explain the mitigation steps to avoid the attacks and, in addition, we discuss the need for changes in the design which will prevent the attacks on SD-WAN in the future. Finally, the concluding section summarizes the key findings of the thesis.

Chapter 2

Background

This chapter gives an overview of enterprise networking history and its existing solutions, along with the drawbacks. Here, we also discuss about the innovative networking technologies that are used in a new alternative, SD-WAN. The SD-WAN architecture and its benefit as an enterprise networking solution are discussed, as well as the necessity for security analysis of SD-WAN solutions. Finally, we provide a brief overview of the literature used as reference for performing the analysis.

2.1 Enterprise networks

Enterprise network is a private network to connect an organization's branches securely for sharing computer resources. The company branches may include company sites, stores, headquarters, and cloud data centers. The enterprise network also forms a communication backbone by integrating all computers, mobiles and other associated devices of an organization. Further, it facilitates interoperability of all these devices within the network. It also improves enterprise data management¹.

An enterprise network can be both local area network (LAN) and wide area network (WAN). Figure 2.1 shows a simple enterprise network with its headquarters, branches and data center connected. Traditionally, enterprise networks used the same telecom networks as voice communication, with very low bandwidth modems to transmit data. However, with the digitization and public internet usage from the 1990s, enterprises started to use virtual private networks that are built over the existing public infrastructure and add encryption to protect the data traffic from eavesdropping. Initially, virtual private network used the frame relay service [10] for providing a private

¹<https://www.techopedia.com/definition/7044/enterprise-network>

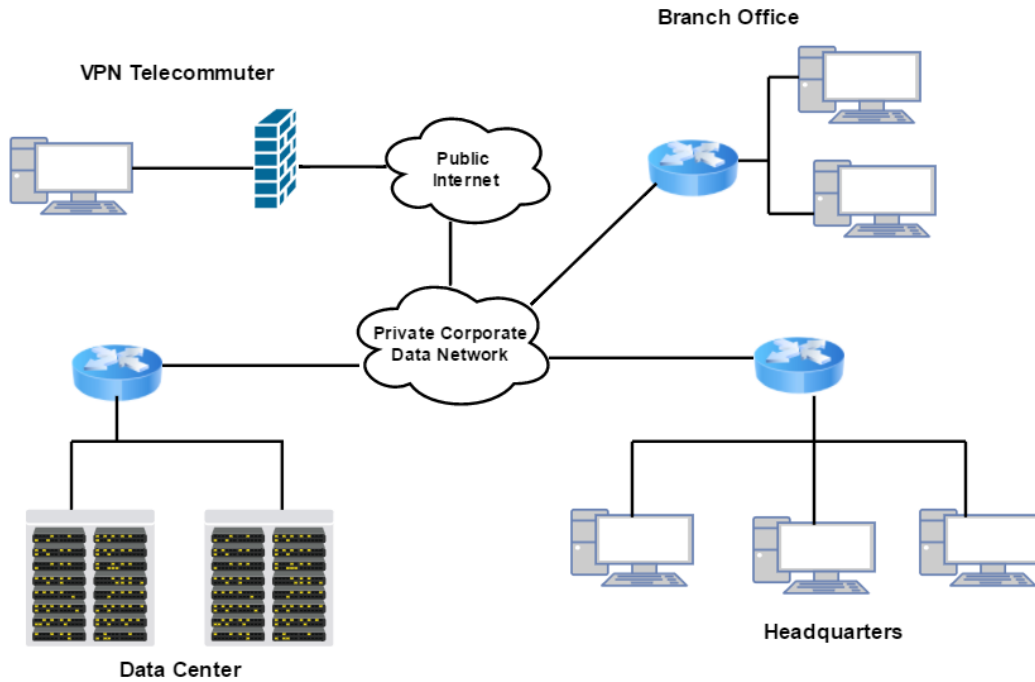


Figure 2.1: Enterprise Network [28]

network. Later, it has been replaced by the MPLS protocol, which is widely accepted and used by all the enterprise networks now.

2.2 Existing MPLS-based networking solution

Enterprise networks started to use the MPLS protocol for their private network from the middle of 2000s. The MPLS protocol increases data speed over the network and improves network's performance. Traditionally, network packets are routed to their destination by routers based on packet's network layer header. A router analyses the IP header and decides where to forward the packet next. Thus, the routing decision is performed at layer 3 of network. With MPLS, the routing decision is made based on assigned labels instead of the IP header. Labels are added to a data packet by an ingress router as it is forwarded to the operator network. Routers analyse the labels and forward the packet to the next router. They do not spend time on analyzing the IP header. Routers usually have set of rules stating where to forward the packets based on their labels. Labels are in the MPLS header, which are prefixed before the IP header. A sample MPLS network

with customer edge routers is shown in Figure 2.2

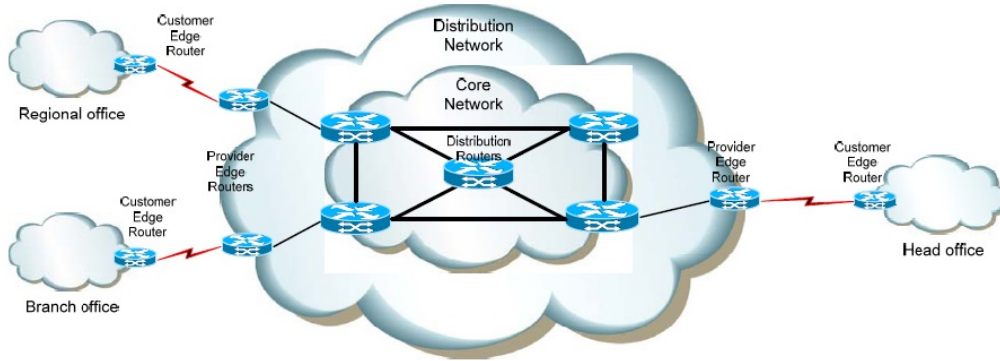


Figure 2.2: MPLS Network [24]

The history of MPLS starts with Ipsilon networks, which proposed a flow management protocol. This protocol works only over Asynchronous Transfer Mode (ATM). Later Cisco proposed tag switching, which is not restricted only to ATM. After some time, Cisco renamed it to label switching and gave it to IETF for open standardization. Then, various vendors started to contribute and, thus it started to work with various technologies such as T1/E1, ATM, Frame Relay, and DSL. Since it works over various networking protocols, it is named as multiprotocol switching.

MPLS has many advantages compared to per-packet routing such as high-speed data transmission, scalability and flexibility to work over any underlying protocol. Because of these reasons, enterprise network widely use MPLS based solutions. Service providers started to provide MPLS based solutions to the enterprises. For example, Sonera in Finland provides a MPLS based solution called Datanet to its customers, and they are a market leader in this business in Finland.

2.3 Problems faced with MPLS

MPLS based solutions are widely accepted by most enterprises for their performance, yet there exists some disadvantages which create the need for new technology. The main disadvantages of MPLS are the costs and adaptation to new technologies such as cloud. The cost of the MPLS based private WAN is higher than the normal internet connectivity cost [11]. Apart from the

cost, deploying MPLS network connection to a new branch location is time consuming. Currently, Sonera takes around 20 days to provide an MPLS connection to a new customer site and it may even take longer depending on the geographic location. The deployment requires manual work in configuring the customer premises router before sending it to the customer location. Further, a network professional is required at the branch location during the deployment which adds to the operations costs.

Enterprises are moving towards the cloudification of their applications. They no longer spend time in setting up the infrastructure for their projects. They offload all their computation, storage and data to the public and private clouds. As enterprises deploy their applications in easily available public clouds such as Amazon AWS and Microsoft Azure, service providers face problems in providing MPLS connection to those public clouds from the enterprise sites. The cloud services can be taken into use within minutes, compared to the weeks of waiting for the MPLS connection. Moreover, some public cloud services may not support MPLS integration.

Further, MPLS is an old technology, which was developed in the 2000s and used for around 16 years. Over this time period, many new networking technologies such as network virtualization and SDN have been developed. Therefore, it is not surprising that new alternatives have been developed to replace this traditional, difficult-to-deploy and expensive MPLS based enterprise network with a more robust and cheaper solution.

2.4 Cutting-edge technologies

As mentioned in the previous section, there is a requirement for new enterprise networking solutions that use all the latest networking technologies. With the evolution of networks over the years, many innovative technologies have been developed which are discussed in this section.

Software-defined Networking

Software-defined networking (SDN) is a new approach for designing, building and managing networks [15]. It separates the network's control from the forwarding plane for better optimization. The simple architecture of SDN is shown in Figure 2.3. It consists of a data plane, control plane and application plane. The network elements are present in the data plane and they focus on packet forwarding. The control plane comprises SDN controllers, and they decide where to forward the incoming packet on the network elements. This decision on the SDN controllers can be controlled by defining rules on

them. Thus, a controller is easily configurable and programmable. These flexibilities in SDN simplify networking.

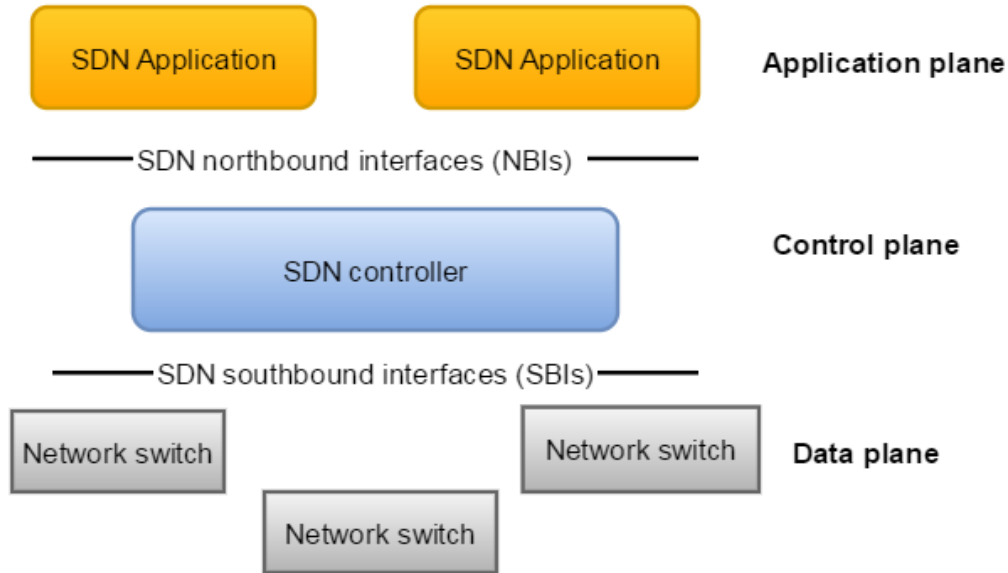


Figure 2.3: Basic SDN Architecture

Network virtualisation

Network virtualization (NV) is the process of converting the network into a software entity known as virtual network, by decoupling the network from the underlying network hardware². It virtualizes the network resources or pathways to achieve application or tenant isolation. In network virtualization, the L2-L7 network services are decoupled from the network hardware and provided as a software to run the virtual network. NV solves many networking challenges especially in data centers where the network needs to be created on demand, without modifying the underlying infrastructure.

Network function virtualisation

Network function virtualization (NFV) is the concept of running a network function in a virtual machine on the virtual server infrastructure [21]. The

²<https://www.sdxcentral.com/sdn/network-virtualization/resources/whats-network-virtualization/>

network functions such as firewall, load balancer and NATs are traditionally run on a customized proprietary hardware and, through NFV, these appliances could be replaced and run on the virtual machines. Usually, the traditional hardware is expensive and results in high dependency on the vendor hardware. However, with the advancements in virtualization technology and increase in the computing power of x86 microprocessors, network functions can be implemented as a virtual application. Thus, NFV reduces the cost and the vendor dependency for the network components.

Cloud computing

Cloud computing is the process of accessing, storing and computing data on data centers over the internet, instead of our local machines. The datacenters can be public, private or hybrid. Cloud computing provides high computing power, high performance and scalability with low cost for the services. Due to the availability of high-speed networks and low-cost internet service, enterprises started to use cloud. It decreases the infrastructure set-up costs for the enterprises as well reduces set-up time where they can focus on their projects instead of infrastructure setup. Cloud providers started to offer pay-as-you-go policies where customers are charged based on their usage. Apart from computing and storage, network solution can also be provided through the cloud by running virtualized network components in the cloud.

Overlay network and its encapsulation techniques

An overlay network is built on top of the existing physical network, connected by the logical or virtual links. This virtual network allows the network resource to be dynamically provisioned and, therefore, it is mainly used in the cloud data centers where the network can be easily managed and provisioned based on the needs. The overlay network also offers programmability of network without changing the underlying network fabrics by adding the intelligent devices at the edges that can be programmed by the controller. These edge devices encapsulate the overlay network packets within the core network packets, forming a virtual network among the edge devices. Thus, the encapsulation plays an important role in the overlay network. There are different encapsulation techniques available such as VXLAN and GRE. Of these, VXLAN is widely used because of its scalability.

VXLAN

Virtual Extensible LAN (VXLAN) is the encapsulation protocol used for running an overlay network on an existing layer 3 infrastructure³. It is mainly used in the WAN and cloud computing environments where isolation of tenants and apps is needed and the virtual networks may extend to many sites over the public IP network. Each tenant in a cloud has its own logical network and network ID, provided by VXLAN. VXLAN is an extension of traditional VLAN, which is used only in the LAN environment because of its limited 4096 network IDs. VXLAN has 16 million unique network IDs that allows this encapsulation technique to function over the WAN also.

2.5 SD-WAN solution

Using the above cutting-edge technologies, a new enterprise network solution, SD-WAN has been developed. This section discusses the SD-WAN architecture and its benefits.

Software defined wide area network (SD-WAN) solution is an internet-based, cloud-enabled networking service, offered to the enterprises. It virtualizes the networking service and eases the complexity of configuring and managing the enterprise network. It is based on the SDN overlay model where the user traffic is encapsulated and then forwarded over the existing network fabrics. The overlay model does not require any change in the existing network fabric; rather it adds the intelligence to the edge device which encapsulates the traffic⁴. The edge devices form a logically separate network on top of the existing infrastructure. The logical network can be formed over any IP network irrespective of the underlying access technologies.

The controller in the control plane controls the edge devices. It acts as a data plane of the network where the traffic is processed as directed by the controller. Figure 2.4 shows the overlay network with edge devices forming a virtual network on top of the physical network. There exists a similar software-defined overlay network in the cloud data centers where the network is virtualized within the datacenter. We extend the same technology for the enterprise WANs across different geographic locations [17]. The edge devices are provided as a customer premises equipment to all the branches and datacenters of the enterprise. A centralized controller controls these CPEs, and the CPEs form a logically separate network using an encapsulation method such as VXLAN or GRE. In addition, encrypting the encapsulated traffic

³<http://whatis.techtarget.com/definition/VXLAN>

⁴<https://www.sdxcentral.com/sdn/resources/what-is-overlay-networking/>

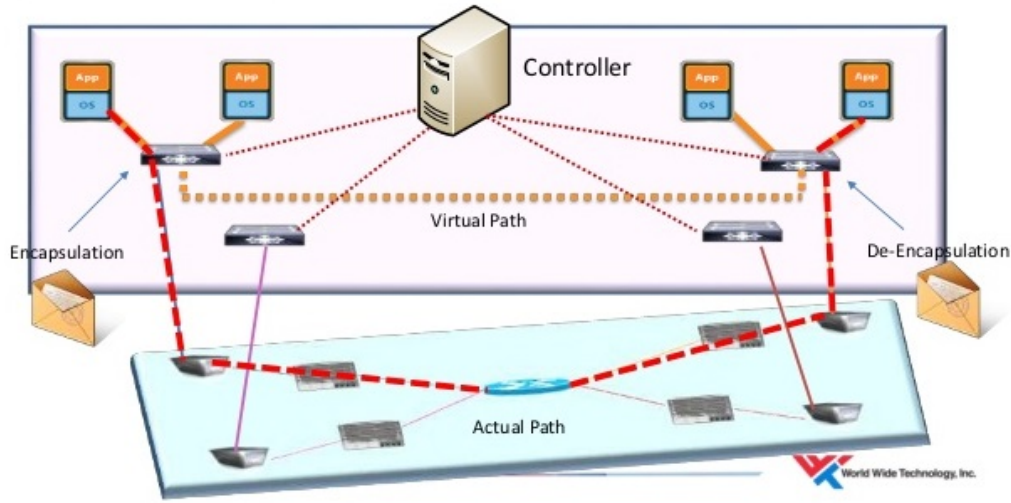


Figure 2.4: SDN Overlay Network [5]

increases security. Figure 2.5 shows the deployment of SD-WAN solution across the different branches and data centers of an enterprise. The SD-WAN solution offers zero touch provisioning of CPEs. Usually CPEs are configured by network professionals at the customer site whereas, in SD-WAN it is provisioned automatically and does not need any network professional at the site. It also offers segmenting of the network, where the customer can choose the types of traffic to be directed over the overlay network and the public internet. Thus, it reduces congestion in the overlay network because enterprise can use it only for high-priority data.

2.6 Need for security analysis of SD-WAN solution

The SD-WAN solution is a replacement for the existing MPLS based network solution. The MPLS based solution is considered reliable and has been provided as a secure enterprise network solution for the past 16 years by service providers. Since MPLS keeps the customer's data separate from the other data streams, it is considered secure and there have been few attacks over the years⁵. On the other hand, SD-WAN uses the insecure public internet for transporting the enterprise data. It uses the latest technologies such as

⁵<http://www.rcrwireless.com/20140513/wireless/mpls-security>

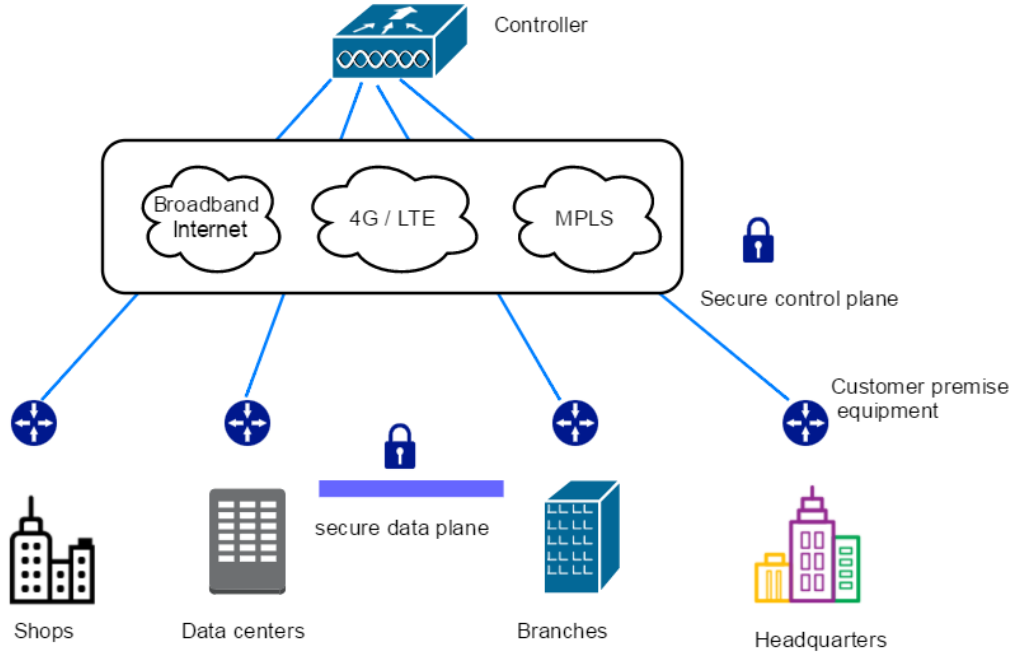


Figure 2.5: SD-WAN Solution

encapsulation and SDN, which are not considered as stable as MPLS in the industry. SDN has many attack surfaces when compared to the traditional network. These article [12][13] list various security attack vectors. SDN's centralized controller is a potential single point of attack and failure [22], and its southbound interface is also vulnerable to the attacks which might affect the availability and performance of the network. Further, SDN allows programmability of the network using its northbound interface. It is always considered as an advantage as it provides more flexibility. However, it also acts as a potential vulnerability where the hackers can trick the engineers to install a compromised application that can reprogram the network [22].

Apart from the SDN weaknesses, vulnerabilities also exist in handling the CPE, which is configured automatically at the customer site. In addition, the CPE is handled and deployed by a non-professional person at the customer site whereas, in MPLS, CPEs are provisioned and deployed by the network professionals, which is more secure when compared to the SD-WAN deployment. Further, enterprises expect a secure and reliable network service for their office sites. Considering all the above factors, there is a necessity to analyze the SD-WAN solution from the security perspective. The outcomes of security analysis will help us realize the vulnerable areas and attack surfaces

of SD-WAN, and these lessons can be used to propose countermeasures for mitigating the attacks in the future.

2.7 Related literature

In the previous sections, we discussed about SD-WAN solution and the need for security analysis for such solution. This section discusses the systematic analysis procedure used while performing security analysis of SD-WAN. We refer to the related literature works that performed similar security analysis.

ONUG SD-WAN working group has released a white paper [27] which provides a set of tactical and strategic requirements for an SD-WAN solution, including the security requirements. The important security requirements, to be considered are listed below.

1. Check the type of encryptions and the encryption algorithms, key length and frequency of key rotation.
2. Check how the security threats such as spoofing, session hijacking and man-in-the-middle attack are handled.
3. Check the PKI (public key infrastructure) implementation and the CA (certification authority) associated with it. Check the process of key generation, distribution and revocation of invalid keys.
4. Check the controller's security and access control for accessing its north-bound API.
5. Check how the AAA (authentication, authorization and accounting) is handled in SD-WAN.

The above requirements are considered during our analysis and we verified whether the given SD-WAN product satisfies them. Many research papers [33] [18] [32] [31] focus on the SDN's controller security and lists the key security issues to be considered while analyzing a controller. Some of the key security issues are unauthorized access, data leakage and denial of service, which have been considered during our analysis on SD-WAN's controller. Then, we focused on the controller's southbound interface that is the OpenFlow protocol in our case. We used [16] [2] [34] as references.

After analyzing the SDN components, we focused on the security of the CPE, which is usually a Linux box. We analyzed the attack surfaces of the CPE as guided in this research paper [19]. This paper analyses and measures the given system's attack surfaces in terms of three kinds of resources:

methods, channels and data. Then, we concentrated on the PKI implementation and the associated certification authority. The hierarchy of CAs and the process of key generation and distribution are examined as in [8]. Generally, misuse of keys and certificates leads to the man-in-the-middle attack [3][4], and we tested the possibilities of such attacks in SD-WAN. Finally, we focused on verifying the access control implemented in the SD-WAN components. Usually, insufficient access control results in attacker acquiring high priority information [30] and, therefore, role based access control has suggested for SD-WAN [39]. As the wider context for our work, we refer to the literature on threat analysis [36][6] and penetration testing [37][9][1].

Chapter 3

Case study:Nuage VNS solution

In the previous chapter, we discussed the significance of SD-WAN for the enterprise networks and the need for security analysis for such solutions. In this chapter, we will do a case study of Nuage VNS, which is one of the SD-WAN solution available in the market. Our case study involves learning the architecture of Nuage VNS and then analyzing them from the security perspective. As a result, we found some vulnerabilities and performed some attacks, which are explained in the following chapter. We used Nuage VNS version 3.2 release 6 for our analysis.

We divide this chapter into two sections where the first section explains the Nuage VNS architecture and its operation, and the second section describes the outcomes of our analysis on the security features of Nuage VNS.

3.1 Nuage VNS architecture

Nuage VNS is an SD-WAN solution offered by Nuage networks. It provides a secure WAN connection between the sites and the datacenters of an enterprise, using the cutting-edge technologies such as VXLAN, SDN and NFV. It is based on the SDN overlay model that provides connection between the sites using any IP network. Since only an IP network is needed, it provides connection between any sites regardless of the service provider and the available access technologies. Thus, it gives more flexibility as we can deploy it in any customer location irrespective of its geographic location or the operator of the access network. The main components of Nuage VNS are the virtualized services directory, virtualized services controller and network services gateway (NSG). Figure 3.1 shows the components of Nuage VNS.

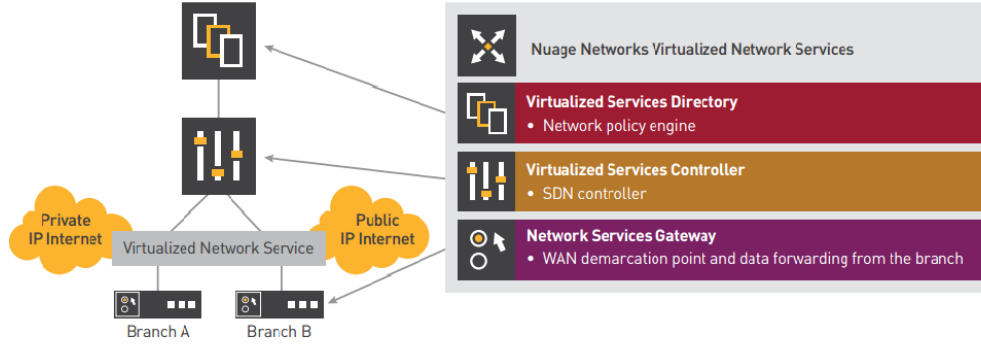


Figure 3.1: Nuage VNS Architecture [25]

Virtualized services directory

Virtualized services directory (VSD) is the centralized policy engine that manages all the components of Nuage VNS solution. It defines rules and policies to all the NSGs located at the different enterprise sites. It is a programmable and analytics engine where the network policies can be easily managed. It allows adding and moving new NSGs to the network via a graphical user interface. Apart from the GUI, there is an API through which network admin or user can manage the network services. VSDs can be deployed as a single machine or in a cluster depending on the workload and scaling needs.

The VSD also acts as a statistics server where the network traffic statistics across the sites are collected. These statistics are aggregated over hours, days and months and stored in a Hadoop analytics cluster to facilitate data mining and performance reporting [26]. Further, VSD manages the security policies for all the NSGs. It also has an network function store from where user can select the network functions needed for their service. Network functions include services such as firewall, DNS and DHCP.

Virtualized services controller

The Nuage virtualized services controller (VSC) is the SDN controller of the Nuage VNS product. It acts as a robust control plane for the network services and maintains a complete view of network topologies and services. It has a northbound and southbound interface. The northbound interface can be accessed by VSD through the XMPP protocol. Apart from VSD, no other component can access the northbound interface of VSC. The south-

bound interface uses OpenFlow protocol to access the NSGs that act as a data-forwarding plane. VSC uses customized OpenFlow messages for programming the Open vSwitch residing in NSGs.

To provide redundancy and scalability, multiple VSC instances can be instantiated within or across the network. The multiple VSC instances communicate through the Multiprotocol Border Gateway Protocol (MP-BGP). MP-BGP is an extension to the Border Gateway Protocol (BGP) that enables BGP to carry routing information for multiple network layers and address families [14]. It is a secure and highly scalable network technology to increase the number of VSC instances according to the business requirements.

Network services gateway

Network services gateway (NSG) constitutes the data-forwarding plane for the customer's network. It acts as a customer premises equipment (CPE) which is placed in the different customer sites such as headquarters, branches and private data centers. NSG is available as both physical hardware and virtual software. Physical hardware is placed in the branches and headquarters whereas virtual NSG software is installed in the public and private clouds. NSG has an Open vSwitch that contacts the VSC through the OpenFlow protocol. VSC applies the network policies, defined by VSD, to NSGs through OpenFlow messages.

The NSG is deployed at the customer sites using an automated process called bootstrapping. Once bootstrapped, it creates an overlay virtual network with the other NSGs of the enterprise. Then it encapsulates and de-encapsulates user traffic, enforcing Layer 2 to Layer 4 network policies as defined by the VSD [26]. Further, encryption is also performed by NSG through IPsec. Service chaining can be instantiated at NSG by defining a service policy in VSD. Service chaining includes services such as firewall, DHCP and DNS.

Other components

The other important components of Nuage VNS are key server, certification authority, notification application and proxy. The key server resides in the VSD and it generates the cryptographic keys and seeds needed for the NSG to encrypt user traffic. The configurations of the key server are managed by the admin through VSD. Certification authority (CA) is a public key infrastructure that issues certificates to the different components of the Nuage VNS. These certificates are used for authorization and authentication of the

components during their communication. Further, it also verifies the digital certificates coming from the NSGs during the bootstrapping process.

Proxy, a separate entity, acts as an intermediary between the NSG and VSD for bootstrap requests. It intercepts all HTTPS requests between the NSG and VSD. It also serves as a certificate-based proxy offering multiple HTTPS endpoints. The notification application sends the activation mail to the installer through the SMTP server. It also takes care of sending activation code as an SMS to the installer during bootstrapping process. Usually, the notification application is installed in the same machine as the proxy.

3.1.1 Nuage VNS operation

VSD and VSC are deployed within the service provider's private trusted network. These software components can be installed in the virtual Linux machines running in the cloud such as OpenStack or VMware. NSG is a customer premises equipment (CPE), which is placed in the customer's branch location. NSG, located in the customer site, communicates to VSD and VSC through the public internet. Apart from the physical NSG, we also have a virtual NSG, which is placed in the datacenter or private cloud of the enterprise. These physical and virtual NSGs ensure secure communication among the branches and data centers of an enterprise. Figure 3.2 shows the Nuage VNS based wide area network with NSGs deployed in the various branches and data centers and private clouds of an enterprise.

On ordering, physical NSG boxes are delivered to the customer sites by the service provider. The delivered NSG boxes are then deployed at the customer sites by an automated process called as bootstrapping. Whenever NSG is connected to the network at the customer site, the bootstrapping process is initiated. It allows NSG to connect and authenticate itself to VSD by a two-factor authentication method. After successful authentication, NSG connects to VSC and brings up a new customer site in the enterprise network. All devices behind the NSG are now connected to the enterprise network. Since the bootstrapping process is simple and automated, it does not require any network specialist to be present at the customer site. Any non-professional in the customer site can perform the bootstrapping. After the bootstrapping, NSG establishes a VXLAN overlay network connection with the NSGs of the other branch sites belonging to the same enterprise. It encapsulates all its user traffic, enforcing Layer 2 to Layer4 network policies as defined by the VSD. To ensure secure enterprise communication, it also encrypts the user traffic before forwarding to other NSGs. As mentioned in Section 3.1, NSG forwards the traffic based on the network policies enforced by VSD. VSD can enforce policies such as traffic offloading where the NSG forwards

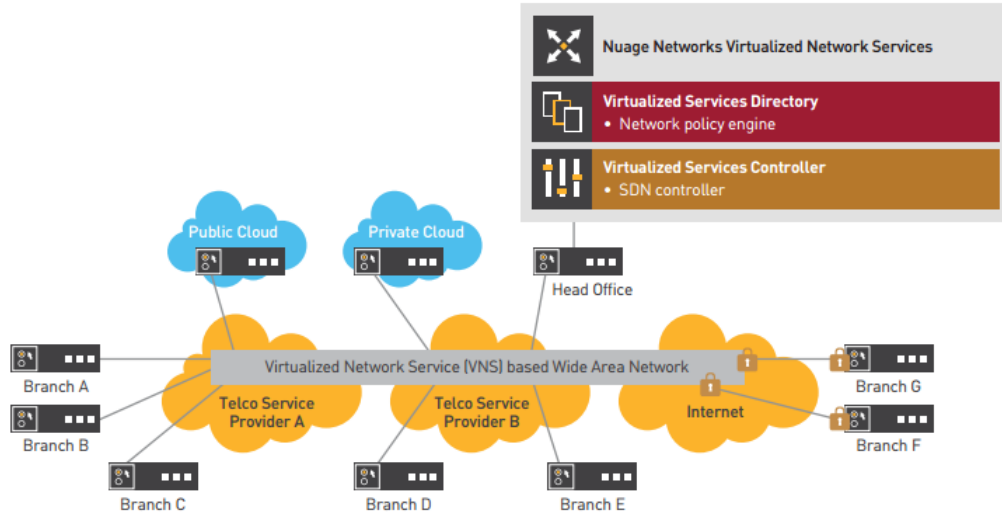


Figure 3.2: Nuage VNS Deployment [25]

the sensitive enterprise data traffic through the secure overlay network and the remaining user traffic can breakout locally through the public internet connection. This increases the bandwidth of the overlay network. Apart from the network policies, advanced network services such as firewall and load balancing can be also enforced in the NSG through VSD.

3.2 Nuage VNS security features

We discussed the architecture and operation of Nuage VNS in the previous section. This section explains the security features implemented by the Nuage VNS and the results of our analysis on them.

3.2.1 Interfaces of Nuage VNS

The Nuage VNS solution has several different components and various communication interfaces between them. Some of the interfaces are open in the internet, which might be vulnerable to attacks. Thus, we studied all the interfaces of Nuage VNS and the communication protocols associated with them. Further, we also verified that each connection between the Nuage components is encrypted and authenticated.

The main communication protocols used are XMPP, OF-TLS and HTTPS. The XMPP protocol is used between the VSC and the VSD as shown in Figure 3.3. XMPP¹ (eXtensible Messaging and Presence Protocol) is based on the extensible markup language (XML) and is used mainly in instant messaging applications. It exchanges messages instantly between any two network entities. VSD communicates the OpenFlow rules and the security policies to VSC through XMPP. Later VSC applies these policies to the respective NSGs. We found that this connection is encrypted and authenticated. It uses TLS connection over XMPP. The required certificates and key pairs for TLS are generated by the VSP CA during the installation. Thus, it is hard for the attacker to intercept this XMPP connection between the VSC and VSD. Further, this connection lies within the service provider's private trusted network, which ensures that this connection is secure.

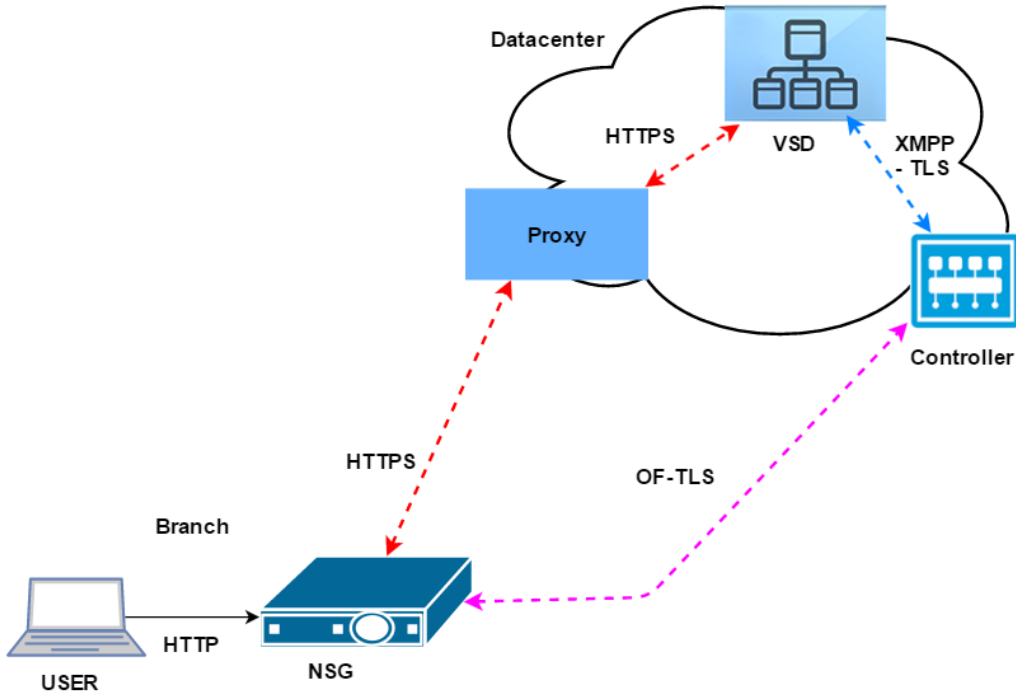


Figure 3.3: Nuage VNS Interfaces

OF-TLS is the OpenFlow over TLS connection protocol that is used between the NSG and the VSC. VSC communicates the OpenFlow rules to the Open vSwitch residing in the NSG through OF-TLS protocol. Since NSG

¹<https://xmpp.org/>

communicates with VSC on the customer site, this connection is established through the insecure public internet. However, this interface is authenticated and data sent over this connection are always encrypted. The encryption uses the VSP CA's certificates and key pairs present in the NSG and the VSC. Open vSwitch, which resides in the NSG, is customized and uses proprietary OpenFlow messages. Thus it is hard for the attackers to read this connection.

HTTPS is a standard HTTP over TLS connection, which is used between the NSG, proxy and the VSD. This connection is initiated mainly during the bootstrapping process where NSG queries VSD via the proxy for certificates and configuration. NSG authentication is also performed through this HTTPS connection. Once authenticated, VSD sends the VSP CA certificates, key pairs and configuration information through this connection. We have two HTTPS connections between the proxy and NSG, one over port 12443 and other over 11443. Each uses its own set of certificates and key pairs while establishing a HTTPS connection.

Thus, all the interfaces between the VNS components are encrypted, authenticated and therefore appear to be well protected from the outsiders.

3.2.2 NSG and the bootstrapping process

NSG is a Linux box with the Red Hat operating system. It has a customized Open vSwitch, which talks to the Nuage controller, once activated. NSG box has six ports that include one WAN port and LAN ports. During dual uplink scenario, LAN port1 can also act as a WAN port. NSG is connected to the internet by the WAN port. Devices at the customer site are connected to one of the LAN ports in order to join the enterprise network. Figure 3.4 shows the real NSG box along with its physical ports. We can log into the NSG box through SSH on port 893. It allows only the nuage user with the default factory-set password. For security purposes, the nuage user has been given only few privileges and it can execute only a minimal commands on the NSG box. There is also a root user whose password is known only to the device vendor. He has more privilege and can access all the commands. Since the root user has more privileges, we tried to crack the root password in order to analyze its strength. We used John the Ripper password cracker tool² with the hash of root password as an input. The root password hash is obtained from the shadow file in the NSG. However, the tool failed to crack the password, which indicates that the root password is strong and secure.

NSG is delivered to the customer site without any pre-configuration. It is configured only at the customer site by a process called bootstrapping. The

²<http://www.openwall.com/john/>

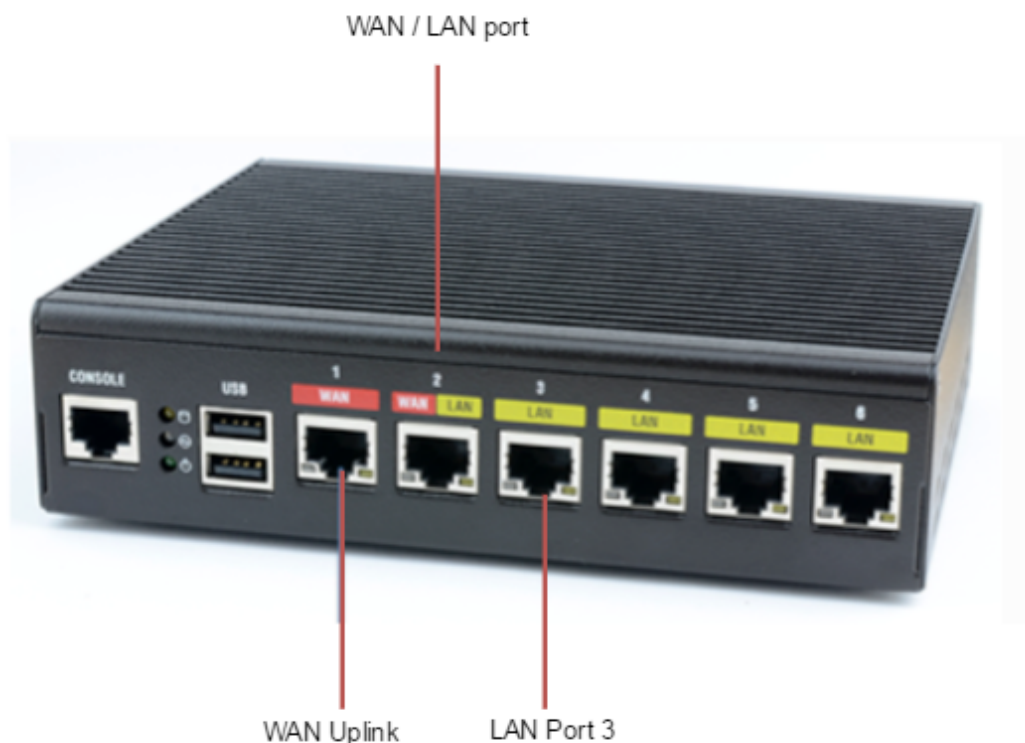


Figure 3.4: NSG box

bootstrapping process allows NSG to securely connect to VSD, download its respective configuration, and connect to the enterprise network. Since there is no pre-configuration, there are chances of bootstrapping NSG from any external network such as the attacker's home network. To avoid such attacks, Nuage VNS has a two-factor authentication process during bootstrapping. The two factors are the installer's e-mail and phone number. Whenever an NSG is ordered, an e-mail is sent to the installer with the activation link. The installer has to connect his computer to port 3 of NSG and start the bootstrapping process by clicking the activation link. On clicking the link, an activation code is sent to the installer's phone number, which has to be entered by the installer to proceed further. This activation code is valid for 60 seconds and thus he has to request for new one if he fails to enter within 60 seconds. Once the correct activation code is entered, NSG is authenticated and continues the bootstrapping process by downloading configuration information.

Thus, the two-factor authentication process prevent NSG from bootstrap-

ping in any external network and getting nevertheless connected to the enterprise network.

3.2.3 Control plane security: VSC security

This section analyses the security of VSC that acts as a control plane in the Nuage VNS services. Being a controller, VSC manages the whole data-forwarding plane and plays an important role in managing the network services across the branch sites. In the world of SDN, the security of controller is a major concern as it is a potential single point of attack and failure [22]. There are several attacks possible on the controller [7]. Attackers can also perform a denial of service attack [38] on controller in order to disrupt the network service. Further, the northbound interface of the controller will be the attacker's main target as it allows to degrade and modify the network using programmable APIs [12]. Considering the importance, we investigated the security of VSC in detail, including all its accessible interfaces.

VSC is provided as a virtual machine application, which can be instantiated on the cloud such as OpenStack and VMware. It is built over the Alcatel Lucent's service router operating system. It is a proven, robust and secure operating system as many of the routers in the world are running it. The operating system is hardened in such a way that the user can access only limited commands. VSCs management interface has an industry-standard CLI, which looks similar to SNMP management. Thus, it avoids the critical command execution that may affect the data plane. Further, the VSC northbound interface can be accessed only by the VSD through XMPP-TLS. Apart from VSD, no other third-party application is allowed to access the northbound API, which makes the system robust. The southbound interface uses OpenFlow over TLS. TLS is made mandatory in order to avoid eavesdropping and spoofed OpenFlow messages. VSC also allows redundancy in case of failure of anyone of them.

3.2.4 IPsec key rotation method

NSG performs IPsec encryption of user traffic that traverses over the WAN networks between the branch sites or between the branch and headquarters. We analyzed this IPsec encryption to understand the steps and encryption methods used. This section explains those methods and the security considered in them.

IPsec encryption uses a symmetric key for encrypting and decrypting the user traffic. All NSGs use the same traffic encryption key (TEK) at a time, and these keys are periodically changed by the key server in VSD

using a key rotation method. Since the TEKs are changed periodically, time is synchronized among all NSGs using an NTP server. VSC acts as the NTP server that periodically updates time to all NSGs. This prevents a time mismatch in NSGs which could lead to a failure of the key rotation method. Further, VSC updates time using the OF-TLS connection, which is an encrypted and authenticated connection. This prevents NTP spoofing on NSGs.

To make the key rotation method secure, the TEKs are not directly distributed among the NSGs. Instead, they distribute the following cryptographic materials, seed encryption key (SEK) and seed among the NSGs. SEK is internally generated by the Key Server and it is encrypted using the public key of the NSG, which is generated as a part of bootstrapping process. These encrypted SEKs are stored in the key server for distribution to the NSGs later. The seed is the keying material for generating TEKs in the NSG. The seed material is encrypted using SEK and signed by the key server. It is also stored in key server for later distribution.

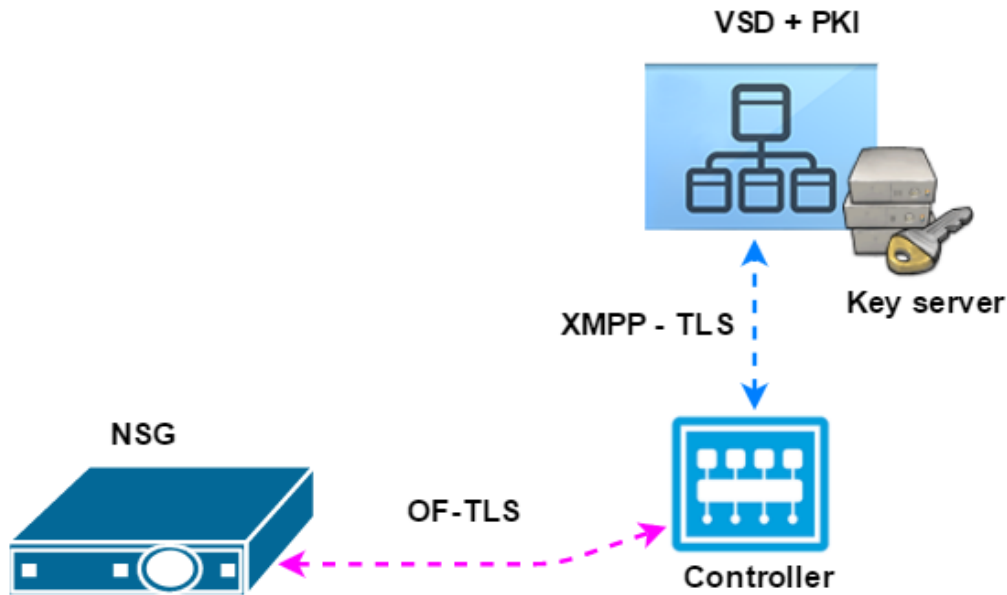


Figure 3.5: Key transport path

The encrypted SEKs and seed are distributed to NSGs in the following steps.

1. The encrypted SEK is first distributed to the NSGs by the key server.

NSG decrypts SEK using its private key and stores it.

2. Now, the encrypted seed is distributed by the key server to NSGs. NSG decrypts the seed using the SEK obtained in the first step.
3. NSG generates TEK using the seed material obtained in the second step. NSG uses a proprietary algorithm to generate TEK from the seed.
4. TEK remains the same across all NSGs at a particular time. User traffic is encrypted using TEK and decrypted by other NSGs using their copy of the TEK.

The SEKs and seed are distributed in the following path as shown in Figure 3.5. It is transported from VSD to VSC over XMPP-TLS and from VSC to NSG over OF-TLS. Both these connections are encrypted and authenticated, which prevents outsiders to access these keys. Further, encryption and signing of the seed material uses updated protocols such as HMAC SHA-1 for authentication, AES256 CBC for encryption, and SHA-256 with RSA for signing. It appears that the IPsec encryption method is secure enough. In case if any NSG is compromised, then the admin can revoke all keys in the NSGs and generate and distribute new SEKs, seeds and TEKs.

Thus, as far as we can see the key rotation method provides secure IPsec encryption of user traffic among the NSGs.

Chapter 4

Vulnerabilities and attack scenarios

We performed security analysis of each component of the Nuage VNS platform and the interfaces among them. The focus of our analysis was primarily on the Network Service Gateway (NSG) since it is available on the customer premises and easily accessible to an attacker when compared to the other components. Further, a non-professional at the branch office handles NSG. He performs the NSGs activation that involves the two-factor authenticated bootstrapping process as mentioned in Section 3.2.2. Despite the two-factor authentication, we suspected potential vulnerabilities and investigated on it further. Thus, our analysis concentrated on the NSG and its bootstrapping process. On detailed enquiry, we found some vulnerabilities in the NSG. Further, we also found some attacks possible on the NSG during bootstrapping process. These vulnerabilities and attacks are explained in this chapter.

Throughout this chapter, we specify three roles: vendor, service provider and customer. The vendor refers to the technology provider, which is Nuage Networks in our case. The service provider refers to operators such as Sonera. Customers are the enterprises who buy the technology and WAN service from the service provider and deploy it at their sites.

4.1 Analysis of NSG attack surfaces

In this section, we look into the attack surfaces of the NSG. We analysed the different possible ways to access this Linux box, NSG. As mentioned in Section 3.2.2, a user can connect to NSG through six physical ports. Apart from these physical ports, we analysed other possible ways to access the NSG

box. We run nmap using Nmap-zenmap GUI tool¹ to find open TCP ports. We found TCP ports 80, 53 and 893 open as shown in Figure 4.1. The nmap result also shows that SSH is open at port 893.

Nmap Output	Ports/Hosts	Topology	Host Details	Scans
<pre> nmap -p1-65535 -T4 -A -v 212.213.61.142 Initiating OS detection (try #1) against 212.213.61.142 NSE: Script scanning 212.213.61.142. Initiating NSE at 15:17 Completed NSE at 15:17, 5.03s elapsed Initiating NSE at 15:17 Completed NSE at 15:17, 0.00s elapsed Nmap scan report for 212.213.61.142 Host is up (0.00062s latency). Not shown: 65531 filtered ports PORT STATE SERVICE VERSION 53/tcp open tcpwrapped 80/tcp open http Apache httpd 2.4.6 ((CentOS)) http-methods: Supported Methods: POST OPTIONS GET HEAD TRACE _ Potentially risky methods: TRACE _ http-server-header: Apache/2.4.6 (CentOS) _ http-title: Nuage Network NSG Activation 443/tcp closed https 893/tcp open ssh OpenSSH 6.6.1 (protocol 2.0) ssh-hostkey: 2048 44:5f:17:58:8f:bd:db:4d:98:29:58:2b:f4:7f:e7:6b (RSA) 256 60:45:23:01:21:95:22:0d:be:01:19:e2:1e:0e:85:30 (ECDSA) MAC Address: 68:54:ED:42:2D:B4 (Alcatel-Lucent - Nuage) Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6.32 OS details: Linux 2.6.32 Uptime guess: 0.015 days (since Tue Mar 15 14:56:45 2016) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=264 (Good luck!) IP ID Sequence Generation: All zeros TRACEROUTE HOP RTT ADDRESS 1 0.62 ms 212.213.61.142 NSE: Script Post-scanning. Initiating NSE at 15:17 Completed NSE at 15:17, 0.00s elapsed Initiating NSE at 15:17 Completed NSE at 15:17, 0.00s elapsed Read data files from: C:\Program Files\Nmap OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 671.28 seconds Raw packets sent: 197118 (8.675MB) Rcvd: 391 (17.945KB) </pre>				

Figure 4.1: Nmap Results

As per the documentation of the product, port 893 is open for SSH for nuage user. Being given limited access, the nuage user can execute restricted commands in the NSG box. SSH is open to the installer when connected through LAN port of the NSG box as shown in Figure 4.2. Apart from port 893, port 80 is also open to the installer. A web server is running in this port and is accessible to the installer when connected to LAN port 3 of the NSG box. Since these open ports are potential attack surfaces, we focussed our analysis on them. As expected, some vulnerabilities were found which are explained in the following sections.

¹<https://nmap.org/zenmap/>

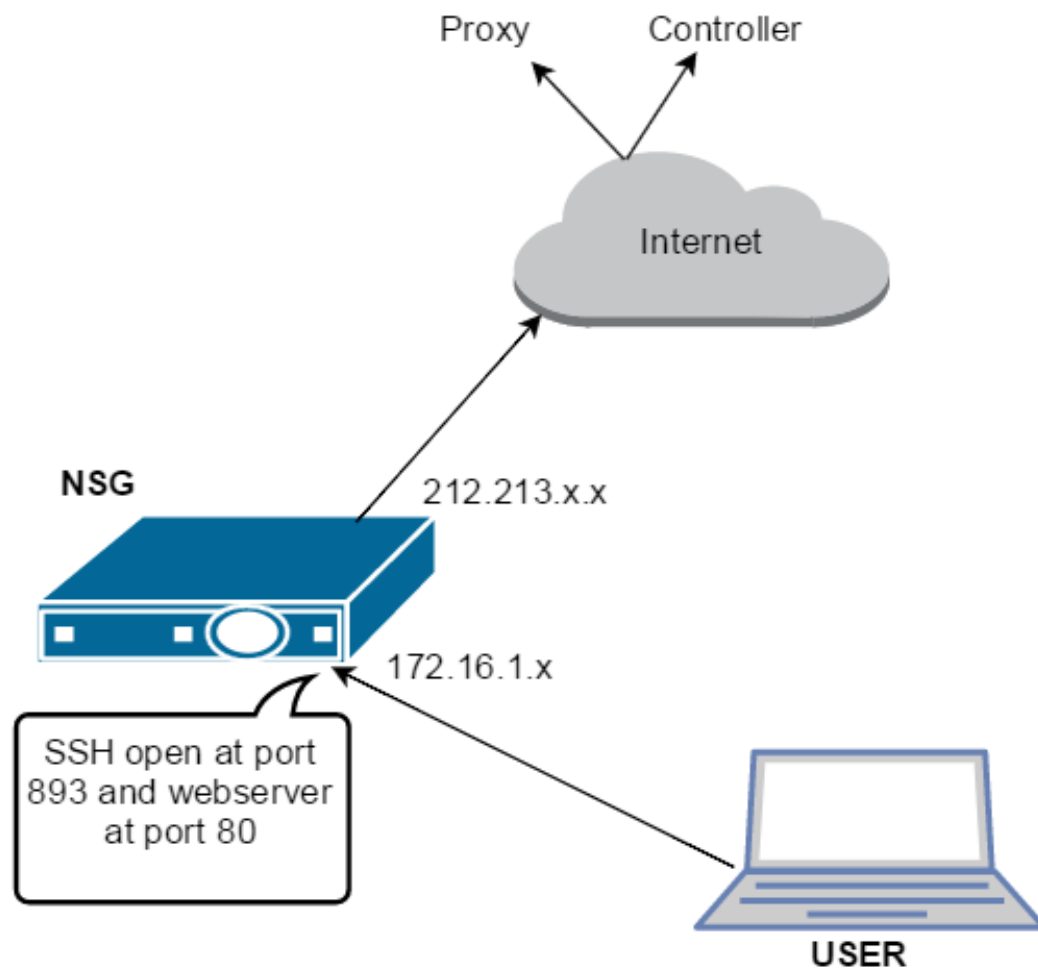


Figure 4.2: NSG at customer site

4.2 Basic vulnerabilities

This chapter explains some of the simple vulnerabilities found in the NSG box. We will explain the vulnerabilities in the increasing order of criticality with the simple ones are explained in the initial sections, followed by the complex ones in the following sections.

4.2.1 Vulnerability 1: open SSH port

On investigation, we found that SSH port on the NSG is open to the internet on the WAN port with the default username and password. Usually, NSG boxes are shipped directly from the factory to the customer site with the default password. The customer has to change the default password on first SSH login. However, most customers do not have any reason to connect with SSH and hence there is a high chance that NSG boxes would be deployed at the customer sites with the default password. Therefore, the attacker can login to those NSGs from any location on the internet. NSG also forces one to change the default password on the first login. Therefore, the attacker will change the default password before the innocent customer changes it. Figure 4.3 shows the NSG with the open SSH port and the attacker accessing it from different location. Once logged in to the NSG, the attacker can access it with the limited nuage user rights.

Attacker could exploit this SSH weakness and perform the attack below. We assume that attacker knows the default password and the range of IP addresses where the NSGs are being deployed.

Attack steps

1. Attacker performs a slow scan of the service provider's IP address space for SSH servers in port 893.
2. Attacker tries to log in to these nodes with the username nuage and the default password.
3. If the login is successful, the attacker sets his own password.
4. Attacker can now access the NSG with the nuage user rights. For example, he can reconfigure the iptables firewall policy of the NSG.

Apart from the nuage user, root user can also login through port 893. Only the vendor knows the root password and the root can perform all operations in NSG. Therefore, the vendors has access to the NSG boxes at the

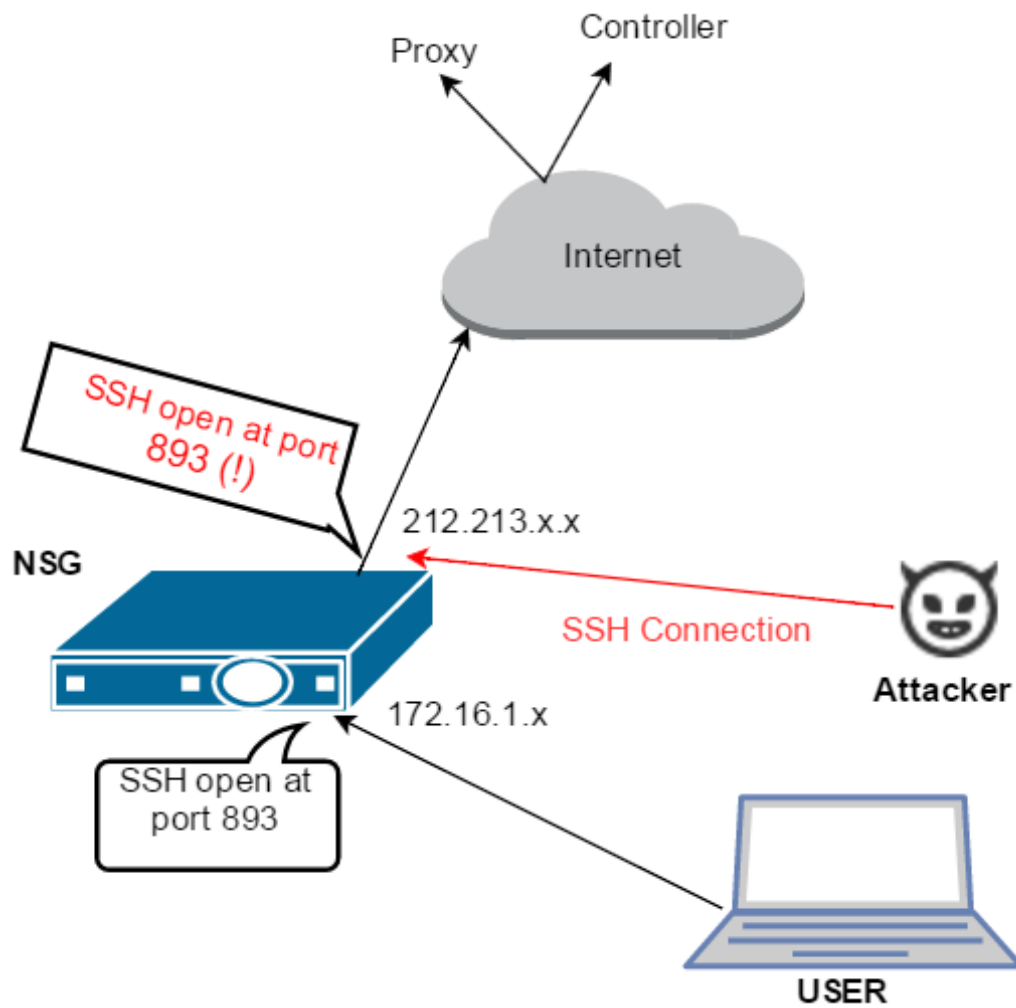


Figure 4.3: NSG with SSH public access

customer sites and can control the customer's network without the help of the service provider.

4.2.2 Vulnerability 2: open HTTP port

The next weakness was in the activation web server, which is open on port 80 of the NSG. According to the Nuage documentation, this web server is accessible to the installer laptop connected to LAN port 3. However, our analysis shows that this web server is open to the internet and can be accessed remotely. Therefore, any remote user can activate the NSG. Figure 4.4 shows this remote activation. Thus, an attacker can activate any NSG without its physical possession.

Attacker could exploit this remote activation weakness and perform the attack below. Here, it is assumed that the attacker knows the IP address of the NSG and he activates it before the innocent customer does it. The attacker should also be a customer of the same service provider and have some NSGs for his own use.

Attack steps

1. Attacker performs a slow scan of the service provider's IP address space for HTTP servers in port 80.
2. Attacker finds an inactive NSG which is going to be activated soon by an innocent customer.
3. Attacker now inactivates one of its own NSGs, starts the reactivation process for it, and receives the activation email.
4. This activation e-mail is used to activate the inactive NSG found in step 2.
5. The NSG and the network behind it will now be connected to the attacker's intranet.

4.2.3 Vulnerability 3: activation e-mail

In this section, we discuss other low priority vulnerabilities found in the Nuage platform.

On analysis of the activation mail sent by Nuage platform to the installer, we found that the activation mail contains data in base64-encoded format.

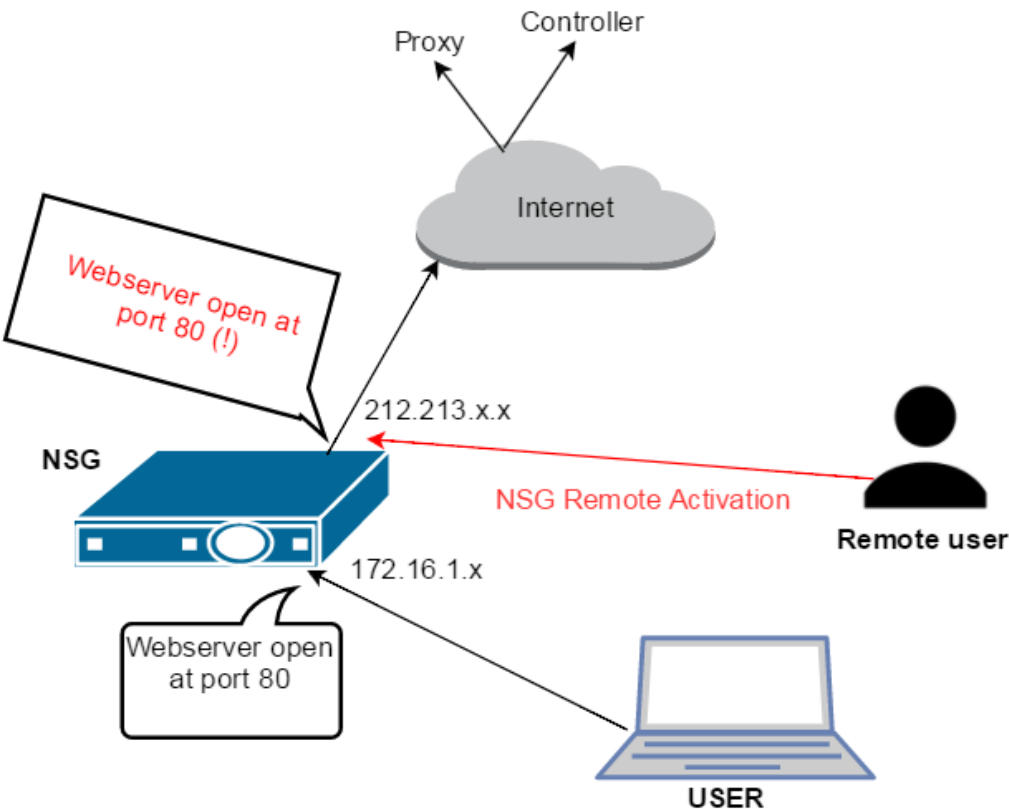


Figure 4.4: NSG remote activation

When we decode the data, we found some critical information such as the installer phone number, e-mail, location of NSG and its UID. Figure 4.5 shows the data available after decoding activation mail.

```
{
  "bootstrap": {
    "id": "fc86a1d7-f144-4add-8982-c127d9ce3f8f",
    "status": "INACTIVE",
    "proxyDNSName": "merry.mit.sonera.com",
    "gateway": {
      "id": "674c2949-4400-4ac1-9c2d-3aa80876cd0e",
      "tpmOwner": "",
      "srk": "",
      "description": "NS Gateway for Ashok",
      "name": "NSG-Espoo-1",
      "systemID": "20.86.109.48",
      "enterprise": "TeliaSonera",
      "enterpriseID": "17f95a68-6e38-4f48-9669-aec13a8cab6c",
      "location": {
        "id": "cbb987a-eedf-4419-a2d6-4868773f01be",
        "address": "Otaniemi, 02150 Espoo, Finland",
        "state": "",
        "locality": "Espoo",
        "country": "Finland"
      },
      "installer": {
        "id": "34d885db-7b1b-4a8a-b674-8d7cc5eca9ad",
        "lastName": "Sonera",
        "email": "admin@sonera.com",
        "firstName": "Admin",
        "mobileNumber": "+358400673713",
        "url": "https://proxy-bootstrap:12443/nuage/api/v3_2/nsgateways/674c2949-4400-4ac1-9c2d-3aa80876cd0e/bootstrapactivations"
      }
    }
  }
}
```

Figure 4.5: Activation mail decoded results

If the attacker hijacks an activation e-mail, he can obtain information about the NSG and its installer. In particular, decoding the activation e-mail reveals the installer phone number to which the activation code will be sent as an SMS. Now the attacker knows the mobile number to be hacked for obtaining the activation code. The attacker may be able to hack the SMS from a mobile in many ways. He can perform social engineering to get the activation code. In social engineering, attacker calls the installer directly and tricks him to reveal the activation code. If the installer believes the attacker, he might tell the activation code. Apart from social engineering, the SMS can also be obtained by installing trojans or apps in the installer's mobile. Many SMS hacking apps such as mspy² and mobile spy³ are available in the market. To install these apps in the installer's mobile, the attacker needs to access the mobile phone at least once. Hacking the SMS is also possible by using SS7 vulnerabilities as mentioned in this whitepaper [29] released by Positive technologies. Another paper [23] about security of SMS based one time password summarizes that one time password over SMS is not secure anymore and there are various attacks possible to crack the one time password. This proves that SMS with activation code is not a strong authentication method anymore. In our case, if the attacker hijacks the e-

²<https://www.mspy.com/>

³<http://www.mobilespy.net/>

mail, he may be able break the second factor SMS by trying one of the above methods.

Further analysis shows that there is no time stamp in the activation mail, which allows activating an NSG with any old activation e-mail that has not yet been used. Thus, the attacker will be successful in his attacks if he hijacks any of the old activation e-mails, provided that the NSG profile associated with that activation mail has not been used or deleted in the Nuage platform yet.

We continued our analysis by modifying the values of the activation e-mail and found that the Nuage platform expects only the UID parameter with the correct value. The remaining parameters can be fake values, and hence the attacker can compose his own e-mail by giving only the correct UID and proxy address. Therefore, the e-mail, the first factor of the two-factor authentication, relies on the UID value. Besides that, the attacker could also tamper the e-mail by modifying the proxy address and UID. This cause a minor denial of service attack for a short interval as the NSG activation depends on the UID value.

Apart from the above vulnerabilities, there are other social factors affecting the security of this system. Social factors refer to mistakes made by human beings while handling the customers. One example could be the scenario in handling big customers. Usually, a big customer orders a large number of NSGs for the customer sites from the service provider. While ordering, they would prefer not to enter the installer's details for all the customer sites and mostly end up filling in only IT admin details. The IT admin receives all the activation e-mails and codes, which would be forwarded to the installers in the different customer sites. Forwarding the e-mails and activation codes is not always a secure way, and attacker could use these circumstances in his favour. The service provider should avoid these kind of batch deliveries while handling big customers.

4.3 Attacks against the NSG bootstrapping process

In the previous section, we discussed various vulnerabilities and attacks on the NSG interfaces. This section discusses the vulnerabilities found in the bootstrapping process. This section is divided into two subsections where the first subsection describes the steps involved in the NSG's bootstrapping process and the weaknesses associated with it, and the second subsection demonstrates the possible attacks on the NSG based on its bootstrapping

weaknesses.

4.3.1 NSG bootstrapping process

Bootstrapping is the initial part of the deployment where NSG securely connects to the controller from the customer site. The installer connected to the NSG at the customer site initiates this process. At the end of a successful bootstrapping process, NSG will become active and the devices connected to it are attached to the respective enterprise network. The main VNS components involved during the bootstrapping process are the proxy and VSD. When the installer is connected to port 3 of NSG and clicks the link in the activation e-mail, NSG initiates an HTTPS connection to VSD through the proxy. The proxy lies between NSG and backend VSD, and acts as an intermediary for the requests coming from the NSG towards the backend VSD. Then, NSG authenticates itself with VSD and downloads all configuration information including the controller details. Finally, it establishes a connection with the respective controller and connects to the enterprise network. The Nuage VNS architecture is shown in Figure 4.6, highlighting the components and interfaces involved during the bootstrapping process.

To analyse further, we studied each step of the bootstrapping process in detail. Figure 4.7 shows all the steps between the NSG and the Nuage components during bootstrapping process. NSG initiates an HTTPS connection to proxy on port number 12443. It uses the `nsg-bootstrap` certificate on the NSG side and the `proxy-bootstrap` certificate in server side, which is the proxy. The bootstrap certification authority, a third party CA, signs both these certificates. We do not have information about the origin of the bootstrap CA. Port 12443 is used only for the initial two HTTPS connections between the NSG and proxy. Initially, NSG makes an API call `/initiate` in the first request. VSD responds by generating a code and sending it as the SMS to the installer's mobile number. A notification agent connected to VSD performs this operation. This API call also returns a seed value to NSG. When the installer enters the code received via SMS, NSG initiates a second API call (`/authenticate`) with the hash values of the seed and the code. Additionally, NSG also requests SSL certificates by sending certificate-signing request to VSD. The hash values of the code and the seed are used for authentication. If they are correct, VSD accepts NSG and generates certificates for the CSR. These certificates are generated by the VSP certification authority, which resides in VSD. The generated digital certificates are sent back to NSG. NSG is authenticated now and it contains digitally signed certificates from VSP CA, which is the central certification authority for providing certificates to all VNS components of this operator environment. Since NSG

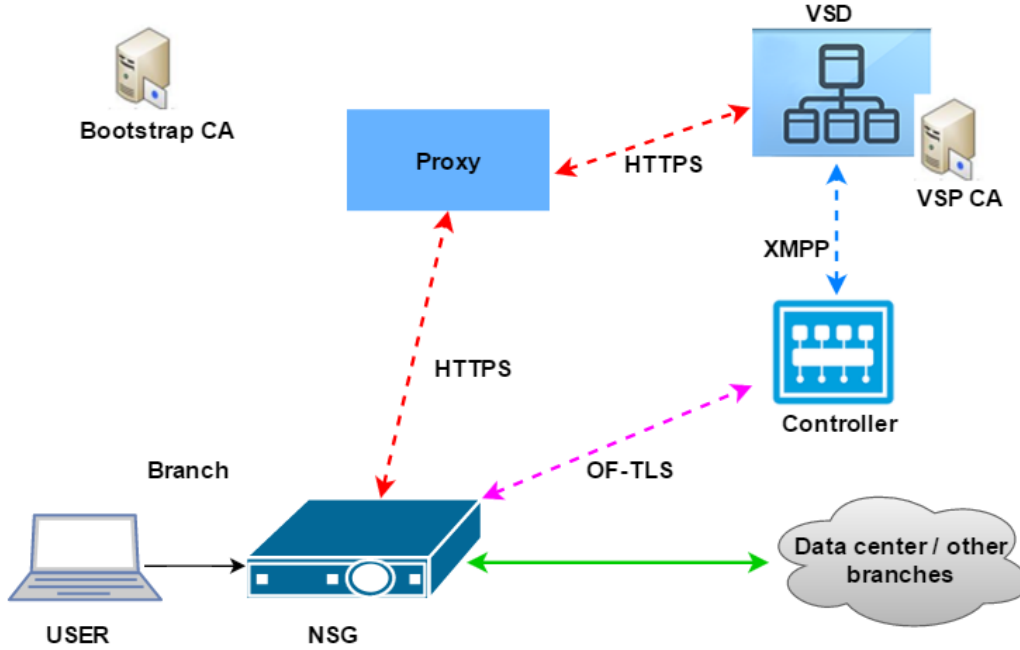


Figure 4.6: VNS Architecture - Bootstrapping process

received the certificate from this CA, it can establish SSL connection to all VNS components of this environment. Subsequent HTTP requests use this new set of certificates for establishing the SSL connection. Now, NSG initiates a new HTTPS connection to the proxy on port number 11443 with the new VSP CA certificates. Then, it makes an API call (`/get.config`) to receive the configuration from VSD. VSD checks the profile of NSG and sends the respective configuration including the controller's details. Now NSG has all the configuration information including the controller to be reached.

NSG initiates an OpenFlow TLS connection to the controller with VSP CA certificates. Once the connection is successful, the controller sends OpenFlow rules to NSG and NSG implements the rules. Local traffic is handled by NSG based on these rules. Thus, the bootstrapping process is successful with the above steps.

After studying all the steps in details, we focused our security analysis on the first HTTPS connection between the NSG and proxy as it involves a third

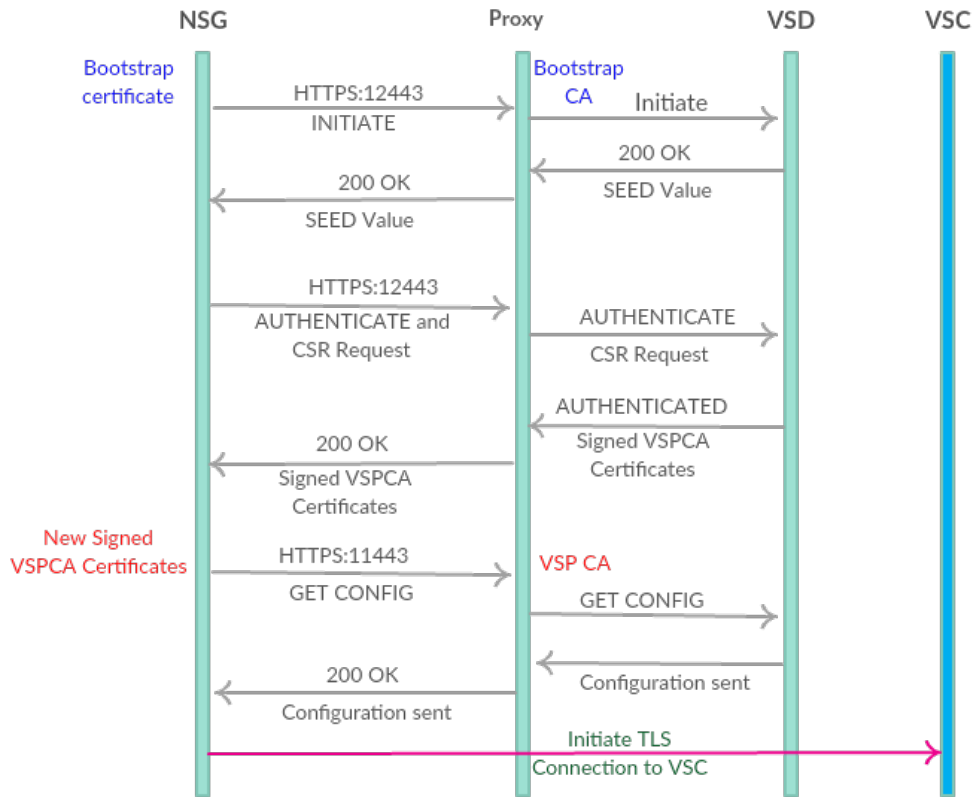


Figure 4.7: Bootstrapping process steps

party bootstrap CA. We started to investigate the origin of the bootstrap certificates and their generation in the NSG and proxy. According to Nuage documentation, NSG devices are not pre-configured and they are delivered to the customer directly from the factory. This shows that bootstrap certificates are loaded as a part of Nuage Red Hat OS image in the NSG box. We tried to access these certificates in the NSG and we were successful in reading and copying them with the nuage user credentials. We were also able to copy the private keys and certificates. We checked a different NSG box for comparison and it contains the same set of bootstrap certificates and private keys. This confirms that all NSGs seem to be pre-loaded with same bootstrap certificates irrespective of the customer.

After NSG, we focused on the proxy and the origin of proxy-bootstrap certificates. According to Nuage documentation, the proxy machine can be any third party proxy such as F5 or a proxy provided along with other Nuage components. The F5 proxy is the preferred one to use in production

environment. On checking the configurations for both the proxies, the F5 proxy configuration document directs to copy the proxy-bootstrap certificate from the VM as shown in Figure 4.8. This confirms that the proxy-bootstrap certificates are not generated but rather copied from the VM given by Nuage. Next, we checked the documentation of the Nuage proxy where we did not find any steps for generating a proxy-bootstrap certificate. This further shows that the proxy-bootstrap certificates come built-in inside the VM. Since the documentation is common for all service providers, we can assume that all service providers use the same proxy-bootstrap certificates. This further proves the point that the NSG boxes are not pre-configured and customised based on the service provider. So irrespective of the service provider, identical NSG boxes are delivered to the customers from the device vendor.

```
Copy (scp) the following certificates needed for bootstrap from the
sdvpn-utils-VM to F5
/opt/SDVPNHAProxy/config/keys/BootstrapCA.pem
/opt/SDVPNHAProxy/config/keys/proxy-bootstrap.pem
```

Note

The proxy-bootstrap.pem file is a certificate bundle that contains the bootstrap-key, bootstrap-certificate and the BootstrapCA files. The client SSL profile on the F5 requires an explicit key and certificate pair and might not accept the CA bundle format. In this case, split the proxy-bootstrap.pem file to generate two new files: bootstrap-key.pem and bootstrap-cert.pem.

Figure 4.8: F5 proxy configuration instructions

We observed that the bootstrap CA certificate and key pair are the same for all service providers. Thus, it is very likely that the attacker gets access to the proxy-bootstrap certificates and keys. For example, the attacker may have an insider working for any one of the service providers that uses the Nuage technology, or the attacker could even establish a service provider and obtain the information directly from the vendor. The NSG bootstrap certificates can also be retrieved from the NSG by the customer by logging in with SSH. Based on these observations, we devised various attacks that are explained in the following sections.

4.3.2 Man-in-the-middle attack

This section demonstrates man-in-the-middle (MITM) attack, which is performed on the proxy and NSG connection. To perform this attack, we assume

that globally the same bootstrap keys are used and the attacker is capable of getting those keys. Based on these assumptions, two types of MITM attacks are possible. They are MITM on-path and MITM off-path attack.

MITM on-path

In this attack, the attacker lies in the same path between the NSG and proxy. If he resides in one of the routers on the path from the NSG to proxy, then he can perform this attack. For example, NSG is delivered to the customer site abroad where a different internet service provider provides internet connection. If that service provider decides to spy on the customer's network, they could place the MITM tool in one of the routers that provide access to the customer. All IP packets from the customer site have to pass through this router. This MITM tool contains both proxy-bootstrap and NSG-bootstrap keys. It acts as both a proxy and NSG in the middle. Whenever NSG initiates an HTTPS request to the proxy on port 12443, the MITM tool terminates this request and initiates a new request to the proxy. The proxy responds to this request, which will be intercepted by the MITM tool and directed back to NSG. The sequence of the bootstrapping process after setting the MITM tool in the middle is shown in Figure 4.9. We performed this attack with an open source MITM tool⁴ and recovered the first two HTTPS request as highlighted in Figure 4.9. The screenshots of the requests captured by MITM tool is shown in Appendix C. Possibly, we could hack subsequent HTTPS requests also, which needs some modification in the MITM tool.

MITM off-path

This attack is performed by forcing the NSG to connect to the attacker's proxy instead of the Nuage proxy. Then the attacker's proxy can initiate a connection to the real Nuage proxy, thus placing the attacker's proxy in the middle. Now it can intercept the HTTPS request between the NSG and proxy. Figure 4.10 shows the attacker's proxy between the NSG and real proxy.

Attacker can force NSG to connect to his proxy in three different ways.

1. The attacker spoofs the activation e-mail sent by Nuage, which contains data in base64-encoded format. Figure 4.5 shows the data after decoding. The result shows the proxy address, and usually NSG connects to this proxy address. The attacker could spoof this e-mail with

⁴<https://mitmproxy.org/>

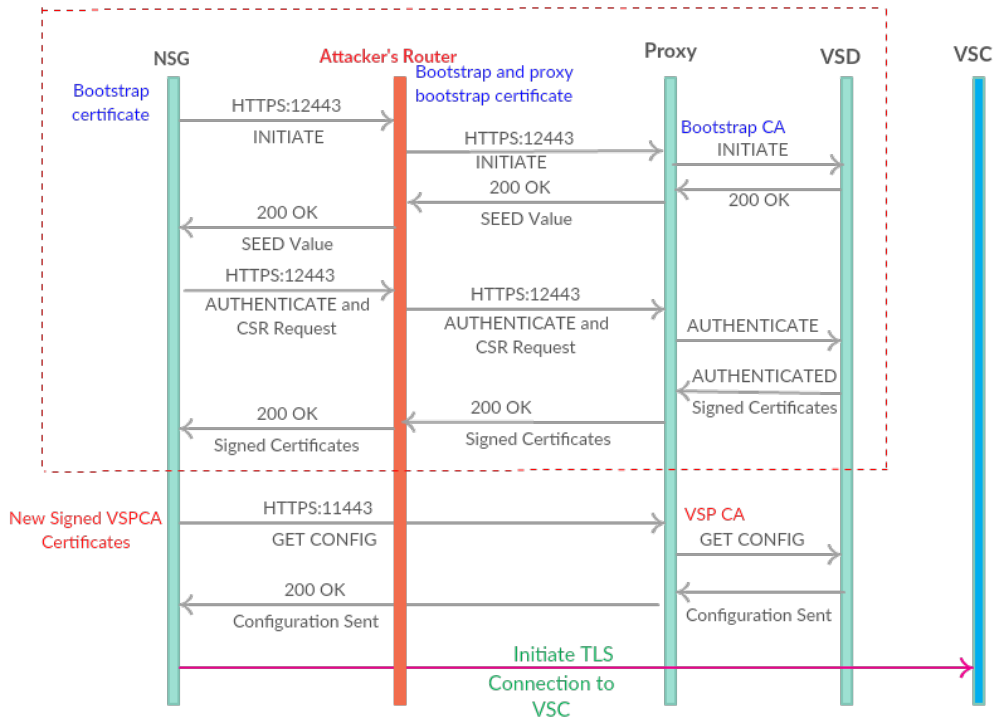


Figure 4.9: MITM attack

his own proxy address. Thus, NSG will be forced to connect to the attacker's proxy, which contains the MITM tool.

2. By exploiting the open SSH port, as explained in Section 4.2.1, the attacker can reconfigure iptables to reroute the connection to its own proxy.
3. With DNS poisoning attacks, the attacker may be able to replace the proxy IP address with its own.

4.3.3 Insufficient access control to APIs

This section explains attacks directed towards the proxy from the attacker's computer. These attacks utilize weaknesses associated with the access control in the backend VSD APIs. The attacker needs the bootstrap client keys and certificates to perform this attack. He acquires these keys from any one of the NSGs of that service provider. He exploits the open SSH port, as explained in Section 4.2.1 and obtains the keys. Attacker should also know the proxy

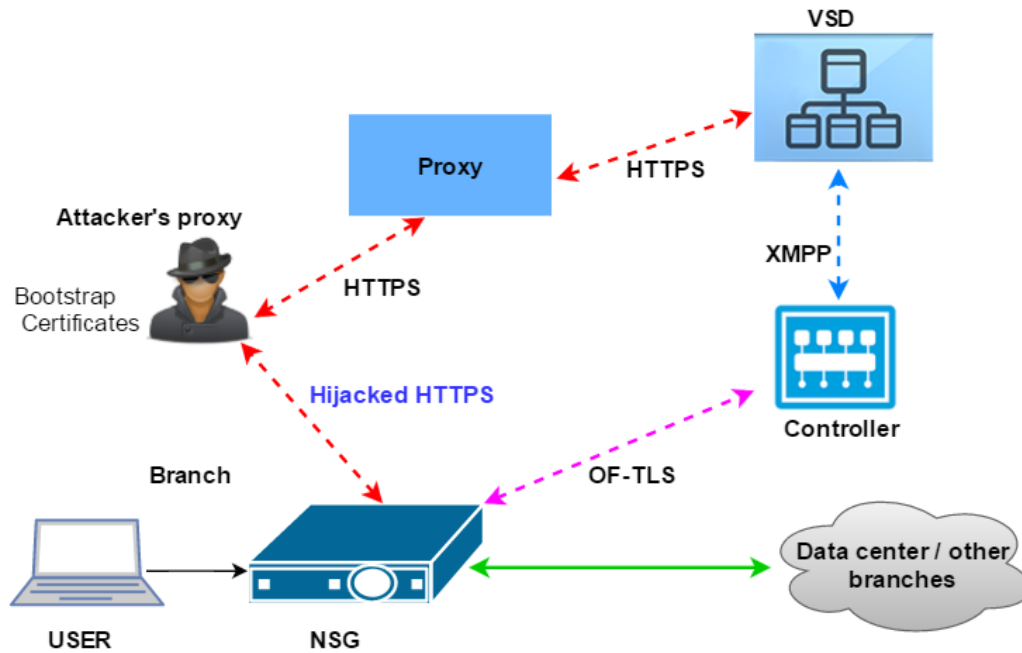


Figure 4.10: MITM off-path attack

IP address in order to establish a connection from his computer. The proxy address can be learnt by decoding the activation e-mails or by spying any one active NSG and its connections or DNS requests.

Once the attacker possesses the bootstrap keys and the proxy address, he can establish the SSL connection to the proxy on port 12443 from his computer anywhere. After establishing the SSL connection, he can access the APIs of Nuage. The sequence diagram in Figure 4.11 shows the connection established between the attacker's computer and the proxy. We performed this attack from our computer, and the SSL connection was successful. Then we tried accessing the APIs and found that we can access critical information that should not be accessible. We were able to collect information such as the enterprise list, installer details, status of all NSGs with their gateway IDs and much more. Apart from getting the information, we were also able to update critical data such as the installer's phone number and e-mail address. Updating the phone number allows the attacker to hack any NSG box, since

it breaks one of the authentication factors in the two-factor authentication method. We updated the phone number and activated NSG without the knowledge of the installer. All of the above information has effect during the bootstrapping process and hence affects only inactive NSGs. We investigated further to find APIs that affect active NSGs and found an API that revokes the active NSGs also. By using this API, any active NSG can be made inactive. Now, the attacker can revoke any NSG in a customer site and bootstrap it again. The list of accessible APIs is documented in Appendix A.

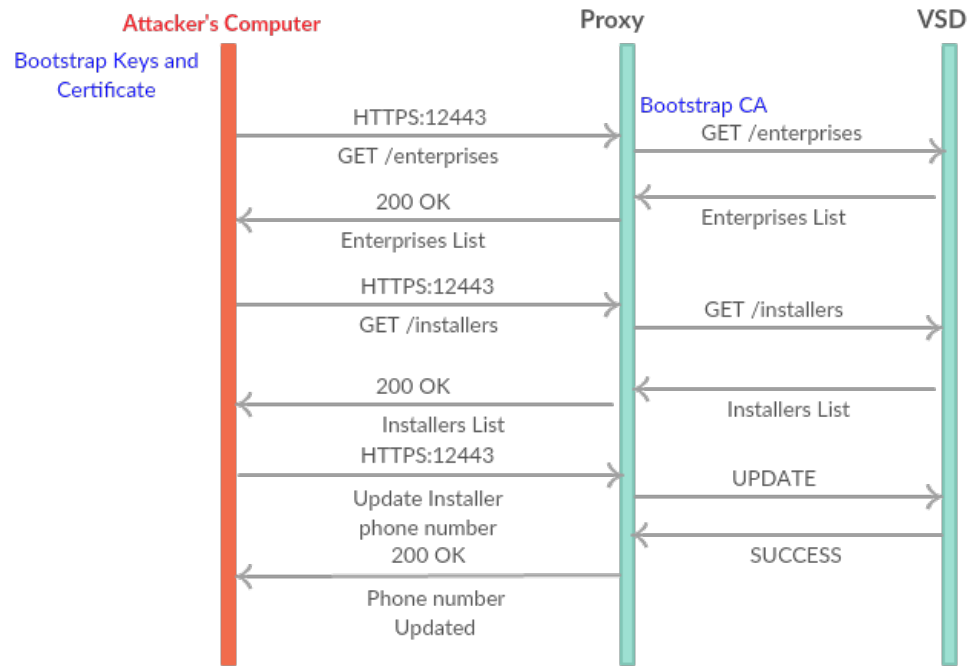


Figure 4.11: Attack on proxy using insufficient access control to APIs

The attacker can perform the following attacks by gathering information using the above APIs. He can remotely join any enterprise network and access their data. Joining the enterprise network is possible in the following two ways.

Physical NSG

Attacker has a physical NSG box and bootstrap keys. If the attacker gets access to any one physical NSG box, he can join any enterprise network using

the above APIs. The attacker needs to know the UID of any one of the NSGs in the enterprise. In addition, he needs to know the installer mobile number associated with that UID. The attacker can get this information by using the APIs described above. Once this information is known, the attacker can initiate the activation of his NSG by composing his own activation e-mail. Through social engineering, as mentioned in Section 4.2.3, the attacker can obtain the activation code from the installer's mobile. If social engineering does not work, still attacker can continue his attack by updating the installer's phone number with the open API. Now the activation code will be sent to the attacker's mobile phone. Thus, the NSG is authenticated and subsequently it joins the enterprise network.

We performed the above attack and were successful in joining the enterprise network with our NSG. The UID used for composing e-mail should be always inactive or else this attack will not be successful. However, we can make any UID inactive using the revoke API and hence this attack will always work.

Emulating NSG

Attacker has only the bootstrap keys. If the attacker has no physical NSG device, it can emulate an NSG in order to join any enterprise network. The attacker emulates an NSG and connects to the real proxy where the proxy considers it as a real NSG and forwards the request to VSD. The attacker's emulated NSG performs all the bootstrap requests and it is authenticated. The attacker uses the same steps as above to break the two-factor authentication and receives the VSP CA signed certificates. Using the VSP CA signed certificates, he gets the configuration of NSG including the controller details. Then, he initiates an OpenFlow TLS connection to the Nuage controller and connects to the respective enterprise network.

We performed this attack using our emulated NSG and successfully established a connection to Nuage proxy. The emulated NSG is authenticated and VSP CA signed certificates are received. Using these certificates, we obtained the NSG configuration and controller details. The controller details include its IP address, public key and certificate. We assume that, with this information, it is possible to connect to the controller using Open vSwitch, which has not been verified yet.

In addition, we found that using these VSP CA certificates, we could obtain the configurations of the other NSGs and access to their information. The possible reason for this behaviour could be lack of access control in VSD, which should restrict NSG's access to the APIs of other NSGs. We mitigated this attack by adding access control at the proxy. After adding

access control rules, the attacker will not be able to access unwanted APIs but still he can access APIs that are required during the bootstrapping. Further, access control did not restrict access to other NSGs information, which can be obtained by using any one of the NSG's VSP CA certificates.

4.3.4 Other attacks

This section describes other attacks that lead to denial of service and confusion among the customers. These attacks make use of the bootstrap weaknesses and the VSD's access control weaknesses explained in the above sections. We assume that the attacker has access to the NSG bootstrap keys and the IP address range of NSGs. In this attack, the attacker revokes the NSG in one enterprise and activates it with the UID of another enterprise. Thus, the customer site belonging to one enterprise is connected to a different enterprise network, which leads to confusion, denial of service, and ultimately giving bad name to the service provider. Here, the NSG is revoked using the revoke API and its activation is possible remotely using its public web server, which is explained in Section 4.2.2. The UIDs and the installer details are obtained and updated by the APIs.

DOS attacks are possible even if the attacker has access only to the proxy bootstrap keys. NSG is forced to connect to the attacker's proxy by tampering the activation e-mail or by updating the iptable rules in NSG. Since the attacker's proxy has proxy bootstrap keys, the connection between NSG and the proxy will be successful. Now the attacker's proxy will simply reply to the NSG's request and even generates and sends a fake activation code to the installer. Then the proxy forces NSG to connect to the fake controller, which sends false OpenFlow rules. The installer assumes that he is connected to the real controller and tries to access enterprise data, which is not possible. This creates confusion and denial of service for a while. This attack can be noticed soon after the installer contacts the operator's customer centre. Nevertheless, a few hours of confusion will cause bad name to the service provider.

Chapter 5

Discussion

We discussed the attacks and vulnerabilities of Nuage VNS in the previous chapter. In this chapter, we discuss the solutions to mitigate the discovered attacks. In addition, we also describe the possible designs that could solve the authentication problem of customer premises equipment. Finally, we propose the future work that can be carried out to proceed further with the security analysis of SD-WAN.

5.1 Solutions for the attacks

The solutions for the attacks and vulnerabilities are listed in this section, in the increasing order of criticality.

5.1.1 Minimizing NSG's attack surface

In order to mitigate the attacks on NSG, we should reduce the NSG's attack surfaces. The main attack surfaces are the open SSH and web server port. These two ports are open to the public internet, which leads to the attacks. These two ports should be closed to the internet and should be made accessible only to the user connected to LAN port 3. Thus, only the installer can access the web server and SSH connection. In addition, the default passwords on the NSGs should be changed before deploying it in the customer site. This can be performed either by the service provider before delivery or by instructing the customer to change the password before deployment. This avoids the attacker logging into NSGs and executing commands.

In addition, we should modify the contents of the activation link sent to the installer. The activation link contains information such as installer's phone number, which could be removed to avoid social engineering attacks.

Further, time validation should be added into the activation link. This prevents the attacker from using old activation links for activation. The activation link should also be made invalid if it is used more than once. The service provider should be careful in collecting installer details such as e-mail and phone number for bigger customers. Correct installer details should be collected and stored in order to mitigate social engineering attacks.

5.1.2 Replacing the bootstrap CA certificates

Bootstrapping attacks are mainly due to the reuse of the certificates provided by the global bootstrap CA. We can mitigate this attack by replacing the global bootstrap CA with the service provider's own bootstrap CA and configuring all NSGs and proxies to trust only this service-provider-specific bootstrap CA. This prevents the attacker's easy access to the bootstrap certificates and related private keys as he needs to access the particular service provider's proxy and NSG for the keys. Still, if he managed to get the bootstrap certificates from that service provider's NSG, he can continue the attacks towards the proxy. We can mitigate this further by configuring all NSGs to have individual names, certificates and key pairs for the bootstrap client. These certificates should also be issued by the service provider's bootstrap CA. Then, in the backend server (VSD), we can keep a mapping of all the NSG names and the respective customers.

In addition, the NSG should restrict access to the bootstrap private keys for the nuage user. This prevents the attackers with SSH access from acquiring the bootstrap private keys without having root access to the NSG.

5.1.3 Adding secure access control at the proxy

Adding secure access control at the proxy restricts access to unnecessary APIs of VSD. Currently, the attacker is able to access APIs because of lack of access control at the proxy. Thus, the proxy machine should be hardened and its configurations should be changed to allow only APIs that are needed during NSG's bootstrapping and post-bootstrapping stage. The vendor should provide this list of APIs and configurations for the proxy.

In addition, we need client certificate authentication to avoid access to other NSG information using any one of the NSGs certificates. Client certificate authentication is a common feature in most of the proxies that lie between the client and backend web server. Usually, the HTTPS connection from the client is terminated at the proxy and the proxy initiates a new connection to the backend web server. Since the client connection is terminated at the proxy, the backend web server does not have information about the

client and its certificates. However, the backend web server needs to know the client identity so that it can perform access control and give permission to access APIs belonging to that particular client only. For this reason, the proxy receives and parses the client certificate and adds this information into one of the HTTP headers sent to the backend server. Now, the backend server receives the client information so that it can perform the access decision. Different proxies do certificate parsing in different ways. Appendix B shows the configurations in F5 proxy and Nginx reverse proxy.

We have this problem in the Nuage platform where the proxy lies between the NSG (client) and VSD (backend server). Since there is no certificate parsing happening in the proxy, there is no access validation at VSD, which enables accessing the configuration information of other NSGs by having a certificate from anyone of the NSG. Thus, we have to add certificate parsing and access control in the proxy and VSD respectively in order to make the APIs secure. That way, the backend server (VSD) API will have fine-grained access control for the requests based on the authenticated NSG name, the list of authorized NSGs, and the mapping of NSGs to customers.

If we make all the above changes, then maybe a simpler NSG activation process would be sufficient because most of the configuration would be already done before shipping the NSG to the customer.

5.2 General discussion

This section discusses the different designs possible for NSG bootstrapping to avoid the authentication problems. The main weakness found in the Nuage VNS is the lack of preconfiguration in the NSG before its delivery. This results in security weaknesses, which lead to the above attacks. In order to perform secure bootstrapping, NSG should be configured before delivering it to the customers. Further, we can also use secure hardware authentication methods such as TPM for CPE authentication. An overview of TPM and its usage in CPEs is given in the following section.

5.2.1 TPM

TPM chips should be used in the CPE for authentication. TPM is a computer chip that securely store the artifacts used to authenticate the platform¹. It provides a hardware based approach for authentication and data protection that improves the security to a higher lever than pure software security. TPM

¹<http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/>

has two RSA key pairs, namely Endorsement Key (EK) and Storage Root Key (SRK). The endorsement key is stored inside the TPM and cannot be accessed or modified by software. The endorsement key is unique to each chip. Storage root key is generated by the combination of Endorsement Key (EK) and the master password entered by admin. Thus, the admin takes the ownership of the hardware. Apart from the admin, no one can access or modify the hardware. TPM uses advanced cryptographic protocols such as RSA, SHA-1, and HMAC². TPM is currently used in laptops, computers and in many types of network equipment for hardware authentication.

TPM can also be used to generate keys and certificates for TLS authentication. Detailed steps for generating keys and certificates are explained in this blog [20]. We can use this feature of TPM for authenticating a CPE which is the NSG in our case. The NSG boxes should be built with the TPM chips having the capability of generating keys and certificates. The installer can claim the ownership of NSG by entering the master password provided by the service provider. This generates unique certificates and keys based on its Endorsement Key. Now, VSD can authenticate the NSG box based on these certificates. Since TPM is used, an attacker would not be able to access these certificates and keys. Thus, the use of TPM prevents the bootstrapping attacks. In addition, the bootstrapped NSGs cannot be claimed by anyone unless they know the master password. However, the security of the master password plays an important role and we should securely distribute the master passwords to the installers.

5.3 Future work

In this thesis, we have primarily focused our analysis on the customer premises equipment, NSG, and its bootstrapping phase. We demonstrated the attacks on the NSG's HTTPS interface. This work needs to continue in the future with an analysis of NSG's OpenFlow interface through which it communicates with the controller. This OpenFlow interface is the southbound interface of controller where the OpenFlow rules are pushed to the NSG. Further, we should verify the possibility of man-in-the-middle attack in the OpenFlow interface and intercepting the OpenFlow messages.

We checked the encryption algorithms and the key rotation method used in the inter-NSG communication. Due to time constraints, we did not spend much time in analyzing the proprietary protocol used in that interface. As a part of the future work, the analysis should continue on these proprietary

²<http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/>

protocols in order to find the possible vulnerabilities. In addition, some of the controller's interfaces also needs to be checked. For scaling, the controller uses the MP-BGP protocol to share information about NSGs. The security of this interface is not analyzed in this thesis, and the work should be done in the future. Further, the northbound interface of the controller, which is VSD's API interface, should be analyzed. Extensive testing is required to check the correctness of access control at VSD.

As a part of this thesis, we analyzed only one commercial SD-WAN solution, Nuage VNS from Nuage Networks. There are many similar SD-WAN solutions available in the market from many vendors such as Huawei and HP. In the future, we would like to perform a similar security analysis of other SD-WAN products provided by major vendors. This analysis will give further knowledge about the possible attack surfaces and the potential vulnerabilities of SD-WAN products in general. This would be helpful in creating general security guidelines to service providers such as Sonera for providing secure SD-WAN service to their customers.

Chapter 6

Conclusions

SD-WAN transforms the future of enterprise networking by providing a flexible and easily manageable network solution to the enterprises. Currently, the enterprises are trying to reduce their operational cost by dropping MPLS links, and the service providers are facing problems in providing MPLS with cloudification support. This trend has led to operators considering SD-WAN as a better solution for the enterprise. However, the introduction of IP-based SD-WAN will increase the risk of potential attacks on the enterprise networks, which are attractive targets for attackers. Hackers are always interested in enterprise networks as they contain valuable computing assets and data. Therefore, both service providers and enterprises consider SD-WAN security as utmost priority, before deploying the new technology widely. In this thesis, we analyzed one such SD-WAN solution, Nuage VNS, and exposed its attack surfaces and security vulnerabilities and finally demonstrated the possible attacks on it.

We first studied about the enterprise WAN networks, various solutions from the past, and the concept of SD-WAN. Its advantages over the past solutions are explained. Further, we also discussed the need for security analysis on SD-WAN and the related literature based on which to perform such analysis. Chapter 3 introduced the SD-WAN product for our case study, Nuage VNS and described its architecture and operation. Then, we analyzed Nuage VNS by investigating its various components and interfaces in detail. As a result, many attack surfaces and security weaknesses were found, especially in the customer premises equipment of Nuage VNS. We also found vulnerabilities in the CPE bootstrapping method and demonstrated some man-in-the-middle attacks by exploiting those vulnerabilities. Finally, we articulated the mitigation strategies to avoid the attacks on NSG and proposed TPM as a starting point for a more secure design that could solve the authentication problems.

The results of the thesis proved that as expected, many new attack surfaces and vulnerabilities can be introduced to enterprise network on providing SD-WAN solution. Considering the magnitude of past attacks on enterprise networks, attackers would easily exploit these weaknesses and cause damage and loss to the enterprises. Thus, both the vendors and the service providers should be aware of these vulnerabilities before providing the technology to enterprises. They should also implement suitable countermeasures to mitigate the attacks as a precautionary step. However, if they ignore these security weaknesses, many attacks on SD-WAN would be witnessed in the future after its wide-scale deployment. We have reported the vulnerabilities in Nuage VNS to the vendor and, based on the constructive response, expect that our work will have a positive effect on the product security.

Bibliography

- [1] BISHOP, M. About Penetration Testing. *IEEE Security Privacy* 5, 6 (Nov 2007), 84–87.
- [2] BRANDT, M., KHONDOKER, R., MARX, R., AND BAYAROU, K. Security Analysis of Software-Defined Networking Protocols OpenFlow, OF-Config and OVSDB. In *The 2014 IEEE Fifth International Conference on Communications and Electronics (ICCE 2014), DA NANG, Vietnam* (2014).
- [3] BURKHOLDER, P. SSL man-in-the-middle attacks. *The SANS Institute* (2002).
- [4] CALLEGATI, F., CERRONI, W., AND RAMILLI, M. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy* 7, 1 (Jan. 2009), 78–81.
- [5] CHANDLER, D. Enterprise Networking Solutions Overview, Jul 2014. Webpage: http://www.slideshare.net/World_Wide_Technology/dave-chandler-presents-sdn-at-world-wide-technologies-tecdav-st-louis.
- [6] CLARK, K., LEE, C., TYREE, S., AND HALE, J. Guiding Threat Analysis with Threat Source Models. In *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC* (June 2007), pp. 262–269.
- [7] DHAWAN, M., PODDAR, R., MAHAJAN, K., AND MANN, V. SPHINX: Detecting Security Attacks in Software-Defined Networks. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015* (2015), The Internet Society.
- [8] DURUMERIC, Z., KASTEN, J., BAILEY, M., AND HALDERMAN, J. A. Analysis of the HTTPS certificate ecosystem. In *Proceedings of the 2013*

- conference on Internet measurement conference* (2013), ACM, pp. 291–304.
- [9] GEER, D., AND HARTHORNE, J. Penetration testing: a duet. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual* (2002), pp. 185–195.
- [10] GOTTLIEB, A. A Brief History of the Enterprise WAN, Apr 2012. Webpage: <http://www.networkworld.com/article/2222089/cisco-subnet/a-brief-history-of-the-enterprise-wan.html>.
- [11] GOTTLIEB, A. Why does MPLS cost so much more than Internet connectivity?, Apr 2012. Webpage: <http://www.networkworld.com/article/2222196/cisco-subnet/why-does-mpls-cost-so-much-more-than-internet-connectivity-.html>.
- [12] HOGG, S. SDN Security Attack Vectors and SDN Hardening, Oct 2014. Webpage: <http://www.networkworld.com/article/2840273/sdn/sdn-security-attack-vectors-and-sdn-hardening.html>.
- [13] JORM, D. SDN and Security, Apr 2015. Webpage: <http://onosproject.org/2015/04/03/sdn-and-security-david-jorm/>.
- [14] JUNIPER NETWORKS. Understanding Multiprotocol BGP, Feb 2014. Webpage: http://www.juniper.net/documentation/en_US/junos15.1/topics/usage-guidelines/routing-enabling-multiprotocol-bgp.html. Accessed Feb 2014.
- [15] JUNIPER NETWORKS. Network Virtual Evolution: Delivering Business Value, Sep 2015. Webpage: http://andicom.co/wp-content/uploads/2015/09/CLAdirect-Network-Virtual-Evolution-v_Final-150901.compressed.pdf.
- [16] KLOTI, R., KOTRONIS, V., AND SMITH, P. OpenFlow: A security analysis. In *2013 21st IEEE International Conference on Network Protocols (ICNP)* (Oct 2013), pp. 1–6.
- [17] KOURLAS, T. Carrier SDN vs Overlay SDN: Duel or Duality?, Oct 2015. Webpage: <https://www.sdxcentral.com/articles/contributed/carrier-sdn-vs-overlay-sdn-ty-kourlas/2015/10/>.

- [18] KREUTZ, D., RAMOS, F. M. V., VERÍSSIMO, P. E., ROTHENBERG, C. E., AZODOLMOLKY, S., AND UHLIG, S. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE* 103, 1 (Jan 2015), 14–76.
- [19] MANADHATA, P. K., TAN, K. M., MAXION, R. A., AND WING, J. M. An approach to measuring a system’s attack surface. Tech. rep., DTIC Document, 2007.
- [20] MAVROGIANNOPOULOS, N. Using the Trusted Platform Module to protect your keys, Aug, 2012. Webpage: <http://nmav.gnutls.org/2012/08/using-trusted-platform-module-to.html>. Accessed Aug 2015.
- [21] MCCOUCH, B. SDN, Network Virtualization, and NFV in a nutshell, Sep 2014. Webpage: <http://www.networkcomputing.com/networking/sdn-network-virtualization-and-nfv-nutshell/1655674152>.
- [22] MCGILLICUDDY, S. SDN security issues: How secure is the SDN stack?, 2014. Webpage: <http://searchsdn.techtarget.com/news/2240214438/SDN-security-issues-How-secure-is-the-SDN-stack?src=itke+disc>. Accessed Aug 2014.
- [23] MULLINER, C., BORGAONKAR, R., STEWIN, P., AND SEIFERT, J.-P. SMS-based one-time passwords: attacks and defense. In *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2013, pp. 150–159.
- [24] NASTECH INC. MPLS data network setup, 2015. Webpage: <http://www.nastechgroup.com/our-services/mpls-data-network-setup/>.
- [25] NUAGE NETWORKS. Extensible Wide Area Networking, 2016. Whitepaper: http://www.nuagenetworks.net/wp-content/uploads/2015/04/PR1503009766_NN_VNS_Extensible_Wide_Area-Networking_Brochure.pdf.
- [26] NUAGE NETWORKS. Virtualized Services Platform, Nov 2014. Webpage: http://www.nuagenetworks.net/wp-content/uploads/2014/11MKT2014097652EN_NN_VSP_Virtualized_Services_Platform_R3_Datasheet.pdf.
- [27] ONUG SD-WAN WORKING GROUP. ONUG Software Defined WAN Use Case, Oct 2014. Whitepaper: https://opennetworkingusergroup.com/wp-content/uploads/2015/05/ONUG-SD-WAN-WG-Whitepaper_Final1.pdf.

- [28] PACKETSTORM COMMUNICATIONS INC. Enterprise Applications, 2014. Webpage: <http://packetstorm.com/enterprise-testing/>.
- [29] POSITIVE TECHNOLOGIES. Signaling System 7 (SS7) security report, Dec 2014. Whitepaper: https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf.
- [30] SANDHU, R. S., AND SAMARATI, P. Access control: principle and practice. *IEEE Communications Magazine* 32, 9 (Sept 1994), 40–48.
- [31] SCHEHLMANN, L., ABT, S., AND BAIER, H. Blessing or curse? Revisiting security aspects of Software-Defined Networking. In *10th International Conference on Network and Service Management (CNSM) and Workshop* (Nov 2014), pp. 382–387.
- [32] SCOTT-HAYWARD, S., NATARAJAN, S., AND SEZER, S. A Survey of Security in Software Defined Networks. *IEEE Communications Surveys Tutorials* 18, 1 (Firstquarter 2016), 623–654.
- [33] SCOTT-HAYWARD, S., O’CALLAGHAN, G., AND SEZER, S. SDN security: A survey. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For* (2013), IEEE, pp. 1–7.
- [34] SHIN, S., AND GU, G. Attacking Software-Defined Networks: A First Feasibility Study. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking* (New York, NY, USA, 2013), HotSDN ’13, ACM, pp. 165–166.
- [35] SOY, S. The case study as a research method, Apr 1997. Webpage: <https://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm>.
- [36] THROWER, W., AND BHATTACHARYA, S. Threat analysis, May 5 2009. US Patent 7,530,104.
- [37] WANG, L., WONG, E., AND XU, D. A Threat Model Driven Approach for Security Testing. In *Software Engineering for Secure Systems, 2007. SESS ’07: ICSE Workshops 2007. Third International Workshop on* (May 2007), pp. 10–10.
- [38] YAN, Q., YU, F. R., GONG, Q., AND LI, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys Tutorials* 18, 1 (Firstquarter 2016), 602–622.

- [39] YUAN, E., AND TONG, J. Attributed based access control (ABAC) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on* (2005), IEEE.

Appendix A

Accessible APIs

1. API call to get enterprises list

```
wget -d -secure-protocol=TLSv1 -certificate=bootstrap.crt -certificate-  
type=PEM -private-key=bootstrap.key -ca-certificate=BootstrapRootCA.pem  
https://proxy-bootstrap:12443/nuage/api/v3_2/enterprises
```

2. API call to get gateway list

```
wget -d -secure-protocol=TLSv1 -certificate=bootstrap.crt -certificate-  
type=PEM -private-key=bootstrap.key -ca-certificate= BootstrapRootCA.pem  
https://proxy-bootstrap:12443/nuage/api/v3_2/gateways
```

3. API call to get status of nsg. We get the json result file where all the parent id's denote the nsg. We can find the active nsg based on creation and last updated date.

```
wget -d -secure-protocol=TLSv1 -certificate=bootstrap.crt -certificate-  
type=PEM -private-key=bootstrap.key -ca-certificate= BootstrapRootCA.pem  
https://proxy-bootstrap:12443/nuage/api/v3_2/jobs
```

4. API call to get installers list

```
wget -d -secure-protocol=TLSv1 -certificate=bootstrap.crt -certificate-  
type=PEM -private-key=bootstrap.key -ca-certificate= BootstrapRootCA.pem  
https://proxy-bootstrap:12443/nuage/api/v3_2/users
```

5. Script to revoke NSG

```
import requests, json  
url="https://proxy-bootstrap:12443/nuage/api/v3_2/nsgateways/{UID}/jobs"  
data = json.dumps( { "ID": "040c714a-51e6-4ec4-8639-43896f195e0f",  
"command": "CERTIFICATE_NSG_REVOKE"})  
cafile = '/home/BootstrapRootCA.pem'  
headers = { 'Content-type': 'application/json' }
```

```
r = requests.post(url, data,headers=headers , verify=cafile,  
cert=('bootstrap.crt', 'bootstrap.key'))
```

Appendix B

Client certificate authentication

Haproxy:

Configurations to be added at haproxy to send client certificate information to backend server are shown below¹.

```
frontend ft_www
bind 127.0.0.1:8080 name http
bind 127.0.0.1:8081 name https ssl crt ./server.pem ca-file ./ca.crt verify required
log-format %ci:%cp [%t] %ft %b/%s %Tq/%Tw/%Tc/%Tr/%Tt %ST %B
%CC %CS %tsc %ac/%fc/%bc/%sc/%rc %sq/%bq %hr %hs {%[ssl_c_verify],
%{+Q}[ssl_c_s_dn],%{+Q}[ssl_c_i_dn]} %{+Q}r
http-request set-header X-SSL %[ssl_fc]
http-request set-header X-SSL-Client-Verify %[ssl_c_verify]
http-request set-header X-SSL-Client-DN %{+Q}[ssl_c_s_dn]
http-request set-header X-SSL-Client-CN %{+Q}[ssl_c_s_dn(cn)]
http-request set-header X-SSL-Issuer %{+Q}[ssl_c_i_dn]
http-request set-header X-SSL-Client-NotBefore %{+Q}[ssl_c_notbefore]
http-request set-header X-SSL-Client-NotAfter %{+Q}[ssl_c_notafter]
default_backend bk_www
```

F5 Proxy:

Client CN can be passed in a HTTP header from the proxy to backend server as shown below².

¹<http://blog.haproxy.com/2013/06/13/ssl-client-certificate-information-in-http-headers-and-logs/>

²<https://devcentral.f5.com/questions/client-certificate-pass-through>

```
# get the CN or user from the subject
set the_user [findstr [lindex $the_cert 2] "CN=" 3 ","]
# copy the username to the header
HTTP::header insert SSL_CLIENT_USER $the_user
```

Nginx reverse proxy:

To send the whole client certificate to backend server for validation, we should add below configuration in the proxy³.

```
proxy_set_header X-SSL-CERT $ssl_client_cert;
```

³<http://serverfault.com/questions/622855/nginx-proxy-to-back-end-with-ssl-client-certificate-authentication>

Appendix C

Snapshots of the MITM tool

The snapshots of the intercepted requests captured by the MITM tool are shown below.

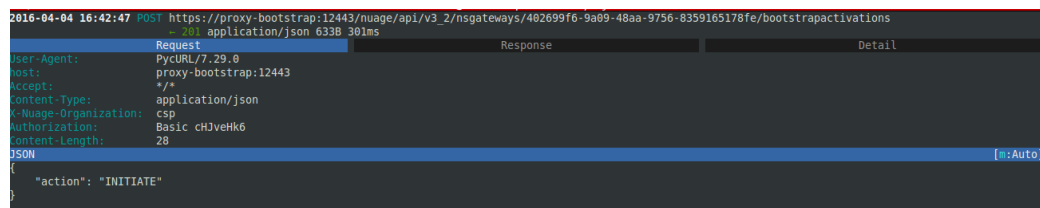


Figure C.1: MITM tool - Intercepted request from NSG

```

2016-04-04 16:42:47 POST https://proxy-bootstrap:12443/nuage/api/v3_2/nsgateways/402699f6-9a09-48aa-9756-8359165178fe/bootstrapactivations
- 201 application/json 6338 301ms

Request Response Detail
Server: Apache-Coyote/1.1
Set-Cookie: rememberMe=deleteMe; Path=/nuage; Max-Age=0; Expires=Sun, 03-Apr-2016 13:42:48 GMT
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: X-Nuage-Organization, X-Nuage-ProxyUser, X-Nuage-OrderBy, X-Nuage-FilterType, X-Nuage-Filter, X-Nuage-Page, X-Nuage-PageSize, X-Nuage-Count, X-Nuage-Custom
Content-Type: application/json
Transfer-Encoding: chunked
Date: Mon, 04 Apr 2016 13:42:48 GMT

JSON [Auto]
{
  "ID": "c65834f7-b7d7-4e4c-904c-2cb1b266e9ef",
  "action": "NEW_NCPE_AUTH_REQUIRED",
  "cacert": null,
  "cert": null,
  "children": null,
  "configURL": null,
  "creationDate": 1459777368260,
  "csr": null,
  "entityScope": "ENTERPRISE",
  "externalID": null,
  "hash": null,
  "lastUpdatedBy": "33a9cef5-fba6-4074-b9ef-80228aa12de3",
  "lastUpdatedDate": 1459777368260,
  "owner": "33a9cef5-fba6-4074-b9ef-80228aa12de3",
  "parentID": "402699f6-9a09-48aa-9756-8359165178fe",
  "parentType": "nsgateway",
  "seed": "arde3d1aldqj9lgj38r96blb9lmeiilslfllpvoh3elusg2qume0q3i7e2h95utrvdqprs3dscv101d43sch8s51lpesf625",
  "srkPassword": null,
  "status": null,
  "tpmOwnerPassword": null,
  "vsdTime": 1459777368260
}

```

Figure C.2: MITM tool - Intercepted response from proxy